AVG Internet Security

Manual do Utilizador

Revisão do documento AVG.01 (9/16/2015)

Copyright AVG Technologies CZ, s.r.o. Todos os direitos reservados.
Todas as outras marcas comerciais são propriedade dos respectivos proprietários.

Índice

1. Introdução **4**

2. Requisitos de Instalação do AVG **5**

2.1 Sistemas Operativos Suportados 5

2.2 Requisitos Mínimos e Recomendados de Hardware 5

3. Processo de Instalação do AVG **6**

3.1 Bem-vindo! 6

3.2 Introduzir o seu número de licença 7

3.3 Personalizar a instalação 9

3.4 A instalar o AVG 10

3.5 Instalação concluída 11

4. Após a Instalação **12**

4.1 Atualização da base de dados de vírus 12

4.2 Registo do produto 12

4.3 Aceder à Interface de Utilizador 12

4.4 Análise de todo o computador 12

4.5 Teste Eicar 12

4.6 Configuração predefinida do AVG 13

5. Interface de Utilizador do AVG **14**

5.1 Navegação da Linha Superior 15

5.2 Informação de Estado de Segurança 18

5.3 Síntese de Componentes 19

5.4 As Minhas Aplicações 20

5.5 Links Rápidos de Analisar/Atualizar 21

5.6 Ícone da barra de tarefas 21

5.7 Conselho do AVG 23

5.8 Acelerador AVG 24

6. Componentes do AVG **25**

6.1 Proteção do computador 25

6.2 Proteção de navegação na Web 29

6.3 Proteção de Identidade 30

6.4 Proteção de E-mail 32

6.5 Firewall 33

6.6 Analisador do PC 36

7. Definições Avançadas do AVG **38**

7.1 Aparência 38

7.2 Sons 41

7.3 Desativar temporariamente a proteção do AVG 42

7.4 Proteção do computador 43

7.5 Verificador de E-mail 48
7.6 Proteção de navegação na Web 63
7.7 Proteção de Identidade 66
7.8 Análises 67
7.9 Agendamentos 73
7.10 Atualizar 82
7.11 Exceções 86
7.12 Quarentena de Vírus 88
7.13 AVG Autoproteção 89
7.14 Preferências de Privacidade 89
7.15 Ignorar estado de erro 91
7.16 Advisor – Redes conhecidas 92

8. Definições da Firewall 93
8.1 Geral 93
8.2 Aplicações 95
8.3 Partilha de ficheiros e de impressoras 96
8.4 Definições avançadas 97
8.5 Redes definidas 98
8.6 Serviços do Sistema 99
8.7 Registos 100

9. Análise do AVG 103
9.1 Análises Predefinidas 104
9.2 Analisar no Explorador do Windows 114
9.3 Análise da Linha de Comandos 114
9.4 Agendamento de Análise 117
9.5 Resultados da Análise 124
9.6 Detalhes dos Resultados da Análise 125

10. AVG File Shredder 127

11. Quarentena de Vírus 128

12. Histórico 130
12.1 Resultados da Análise 130
12.2 Resultados da Proteção Residente 131
12.3 Resultados da Proteção de Identidade 134
12.4 Resultados da Proteção de E-mail 135
12.5 Resultados da Proteção Online 136
12.6 Histórico de Eventos 138
12.7 Registo da Firewall 139

13. Atualizações do AVG 141
13.1 Execução de atualização 141
13.2 Níveis de atualização 141

14. Perguntas Frequentes e Suporte Técnico **143**

1. Introdução

Este manual do utilizador disponibiliza informação completa para o utilizador relativa ao **AVG Internet Security**.

O **AVG Internet Security** proporciona várias camadas de proteção para tudo o que faz online, o que significa que não tem de se preocupar com roubos de identidade, vírus ou visitas a websites prejudiciais. A Rede de Proteção da Comunidade AVG e a Tecnologia de Proteção na Nuvem AVG estão incluídas, o que significa que compilamos as informações relativas às mais recentes ameaças e as partilhamos com a nossa comunidade, para garantir que o utilizador recebe a melhor proteção. Pode fazer compras e realizar operações bancárias online de forma segura, desfrutar de redes sociais ou navegar e pesquisar com a confiança proporcionada por uma proteção em tempo real.

Poderá também querer utilizar outras fontes de informação:

- ***Ficheiro de ajuda***: está disponível uma secção de *Resolução de problemas* diretamente no ficheiro de ajuda incluído no **AVG Internet Security** *(para abrir o ficheiro de ajuda, carregue na tecla F1 em qualquer janela da aplicação)*. Esta secção providencia uma lista das situações que ocorrem com maior frequência e que motivam a procura de ajuda profissional por parte de um utilizador. Selecione a situação que melhor descreve o seu problema e clique sobre a mesma para abrir instruções detalhadas que solucionam o problema.

- ***Centro de Suporte do Website da AVG***: em alternativa, pode procurar a solução para o seu problema no website da AVG (*http://www.avg.com/*). Na secção ***Suporte*** pode encontrar uma visão geral de grupos temáticos relacionados com questões técnicas e comerciais, uma secção estruturada de perguntas frequentes e todos os contactos disponíveis.

- ***AVG ThreatLabs***: um site específico associado ao AVG (*http://www.avg.com/about-viruses*) e dedicado a questões relacionadas com vírus, que apresenta uma síntese estruturada de informações relativas a ameaças online. Também encontra instruções para a remoção de vírus, spyware e conselhos sobre como se manter protegido.

- ***Fórum de debate***: também pode usar o fórum de debate dos utilizadores do AVG em http://community.avg.com/.

2. Requisitos de Instalação do AVG

2.1. Sistemas Operativos Suportados

O **AVG Internet Security** destina-se a proteger estações de trabalho com os seguintes sistemas operativos:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (todas as edições)
- Windows 7 (todas as edições)
- Windows 8 (todas as edições)
- Windows 10 (todas as edições)

(e possivelmente Service Packs superiores para sistemas operativos específicos)

***Nota**: O componente Identidade não é suportado em Windows XP x64. Nesse sistema operativo pode instalar o AVG Internet Security, mas apenas sem o componente Proteção de Identidade.*

2.2. Requisitos Mínimos e Recomendados de Hardware

Requisitos mínimos de hardware para o **AVG Internet Security**:

- Intel Pentium CPU 1,5 GHz ou superior
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) de memória RAM
- 1,3 GB de espaço livre no disco rígido *(para fins de instalação)*

Requisitos recomendados de hardware para o **AVG Internet Security**:

- Intel Pentium CPU 1,8 GHz ou superior
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) de memória RAM
- 1,6 GB de espaço livre no disco rígido *(para fins de instalação)*

3. Processo de Instalação do AVG

Para instalar o **AVG Internet Security** no seu computador, precisa de transferir o ficheiro de instalação mais recente. Para garantir que está a instalar a versão atualizada do **AVG Internet Security**, recomendamos que transfira o ficheiro de instalação do website da AVG (http://www.avg.com/). A secção ***Suporte*** disponibiliza uma síntese estruturada dos ficheiros de instalação de cada edição do AVG. Assim que tiver descarregado e guardado o ficheiro de instalação no seu disco rígido, pode iniciar o processo de instalação. A instalação é uma sequência de janelas simples e fáceis de interpretar. Cada janela descreve sucintamente o que fazer em cada passo do processo de instalação. É apresentada uma explicação detalhada de cada janela a seguir:

3.1. Bem-vindo!

O processo de instalação começa com a janela ***Bem-vindo ao Instalador do AVG Internet Security***:

AVG
Bem-vindo à AVG Internet Security
Idioma:
Português
A proteger milhões de pessoas como você
Ao clicar em "Continuar" ou "Instalação personalizada", está a aceitar o Contrato de Licença de Utilizador Final da AVG, a Política de Privacidade e a instalação de atualizações automáticas futuras referentes a produtos AVG.
Continuar
Instalação personalizada

Seleção do Idioma

Nesta janela pode selecionar o idioma usado para o processo de instalação. Clique na caixa junto à opção ***Idioma*** para fazer aparecer o menu de idioma. Selecione o idioma pretendido e o processo de instalação continuará no idioma selecionado. A aplicação comunicará no idioma selecionado, com a possibilidade de mudar para Inglês, que é sempre instalado por predefinição.

Contrato de Licença de Utilizador Final e Política de Privacidade

Antes de continuar o processo de instalação, recomendamos que se familiarize com os documentos ***Contrato de Licença de Utilizador Final*** e ***Política de Privacidade***. É possível aceder aos dois documentos através das ligações ativas na parte inferior da janela. Clique em qualquer uma das hiperligações para abrir uma nova caixa de diálogo/janela do browser com o texto integral do respetivo documento. Leia atentamente esses documentos juridicamente vinculativos. Se clicar no botão ***Continuar***, estará a confirmar que aceita os

documentos.

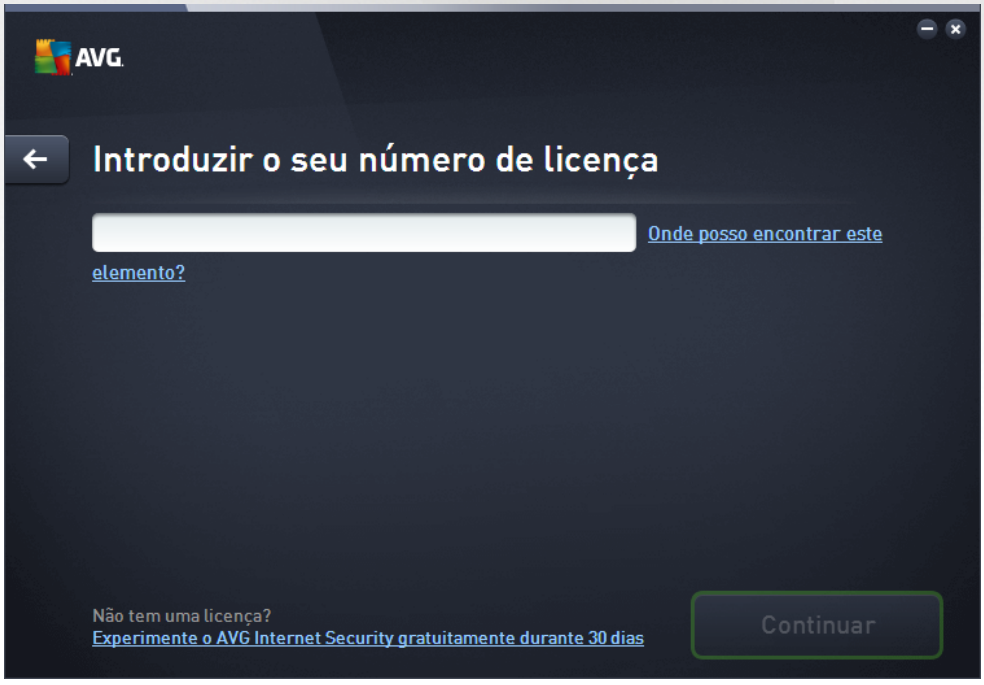
Continuar a instalação

Para continuar a instalação, clique no botão ***Continuar***. Ser-lhe-á pedido o seu número de licença e o processo de instalação será executado em modo totalmente automático. É aconselhável que a maioria dos utilizadores utilize esta opção padrão de instalação do **AVG Internet Security** com todas as definições pré-configuradas pelo fornecedor do programa. Esta configuração proporciona a segurança máxima combinada com uma utilização de recursos otimizada. Futuramente, se houver necessidade de alterar a configuração, tem sempre a opção de o fazer diretamente na aplicação.

Em alternativa, está disponível a opção de ***Instalação Personalizada*** sob a forma de uma hiperligação localizada por baixo do botão ***Continuar***. A Instalação Personalizada só deve ser utilizada por utilizadores avançados que tenham uma razão válida para instalar a aplicação com definições que não sejam as padrão (por exemplo, para corresponder a requisitos do sistema específicos). Se optar por esse tipo de instalação, depois de preencher o número de licença será redirecionado para a janela ***Personalizar a instalação***, na qual pode especificar as definições pretendidas.

3.2. Introduzir o seu número de licença

Na janela ***Ativar a sua licença*** é convidado a introduzir o seu número de licença no campo de texto disponibilizado:


AVG
Introduzir o seu número de licença
Onde posso encontrar este elemento?
Não tem uma licença?
Experimente o AVG Internet Security gratuitamente durante 30 dias
Continuar

Onde encontrar o número de licença

O número de venda pode ser encontrado na embalagem do CD na caixa do **AVG Internet Security**. O número de licença estará na mensagem de e-mail de confirmação que recebeu depois de comprar o **AVG Internet Security** online. Tem de digitar o número exatamente conforme apresentado. Se o formato digital do

número de licença estiver disponível (*no e-mail*), é aconselhável utilizar o método copiar e colar para o inserir.

Como utilizar o método Copiar e Colar

Utilizar o método ***Copiar e Colar*** para introduzir o número de licença do **AVG Internet Security** no programa assegura que o número é devidamente introduzido. Proceda do seguinte modo:

- Abra o e-mail que contém o número de licença.
- Clique com o botão esquerdo do rato no início do número de licença, mantenha premido e arraste o rato até ao final do número, depois liberte o botão. O número deverá ficar realçado.
- Prima e mantenha premida a tecla ***Ctrl*** e depois prima a tecla ***C***. Esta ação copia o número.
- Aponte e clique na posição onde pretende colar o número copiado.
- Prima e mantenha premida a tecla ***Ctrl*** e depois prima a tecla ***V***. Esta ação cola o número na localização que selecionou.

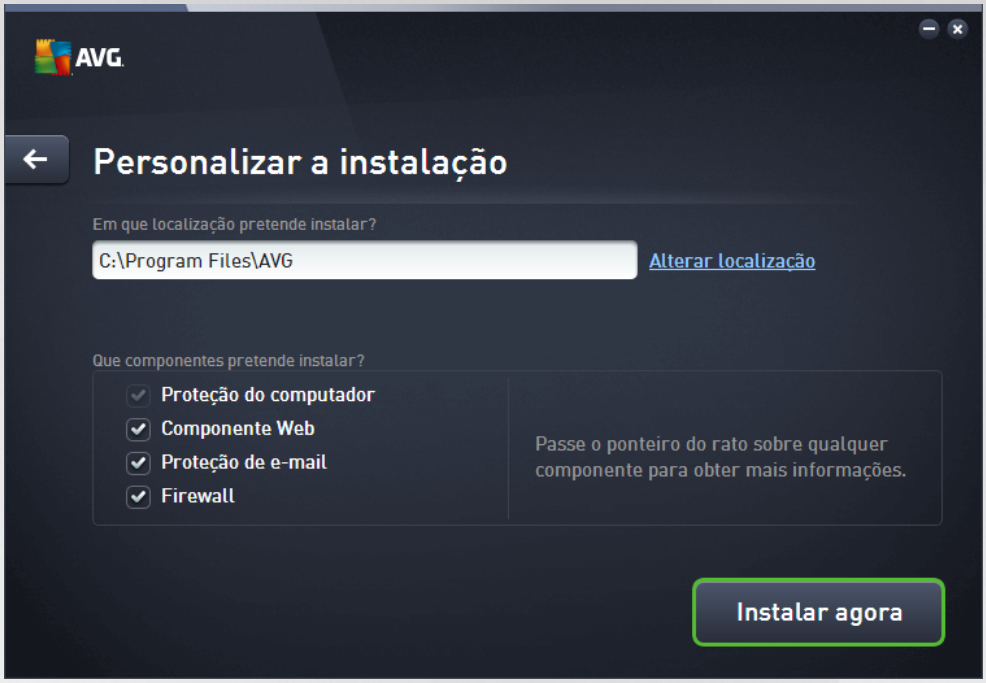
Botões de controlo

Como na maioria das janelas de configuração, há três botões de controlo disponíveis:

- ***Cancelar*** – clique para sair imediatamente do processo de configuração; o **AVG Internet Security** não será instalado!
- ***Voltar*** – clique para retroceder um passo e voltar à janela de configuração anterior.
- ***Seguinte*** – clique para continuar a instalação e avançar para o passo seguinte.

3.3. Personalizar a instalação

A janela ***Opções Personalizadas*** permite-lhe configurar parâmetros detalhados da instalação:



A secção ***Seleção de Componentes*** apresenta uma síntese de todos os componentes do **AVG Internet Security** que podem ser instalados. Se as definições predefinidas não forem da sua conveniência, pode remover/adicionar componentes específicos. ***No entanto, só pode selecionar entre os componentes que estão incluídos na edição do AVG que adquiriu!*** Realce qualquer um dos itens na lista ***Seleção de Componentes*** e será apresentada uma breve descrição do respetivo componente no lado direito desta secção. Para informações detalhadas sobre as funcionalidades de cada componente, consulte o capítulo Síntese de Componentes neste documento. Para reverter para a configuração predefinida pelo fornecedor do software, use o botão ***Predefinição***.

Neste passo, também pode optar por instalar outros idiomas do produto que não os predefinidos *(por predefinição, a aplicação é instalada no idioma que é selecionado como idioma de configuração e em Inglês)*.

Botões de controlo

Como na maioria das janelas de configuração, há três botões de controlo disponíveis:

- ***Cancelar*** – clique para sair imediatamente do processo de configuração; o **AVG Internet Security** não será instalado!
- ***Voltar*** – clique para retroceder um passo e voltar à janela de configuração anterior.
- ***Seguinte*** – clique para continuar a instalação e avançar para o passo seguinte.

3.4. A instalar o AVG

A janela ***Progresso da Instalação*** apresenta o progresso do processo de instalação e não necessita de qualquer intervenção:

AVG
A instalar o AVG Internet Security...
Esta operação pode demorar um pouco
É fácil manter-se protegido
Utilizamos cores e círculos para indicar se está tudo bem

Após a conclusão do processo de instalação, será redirecionado para a janela seguinte.

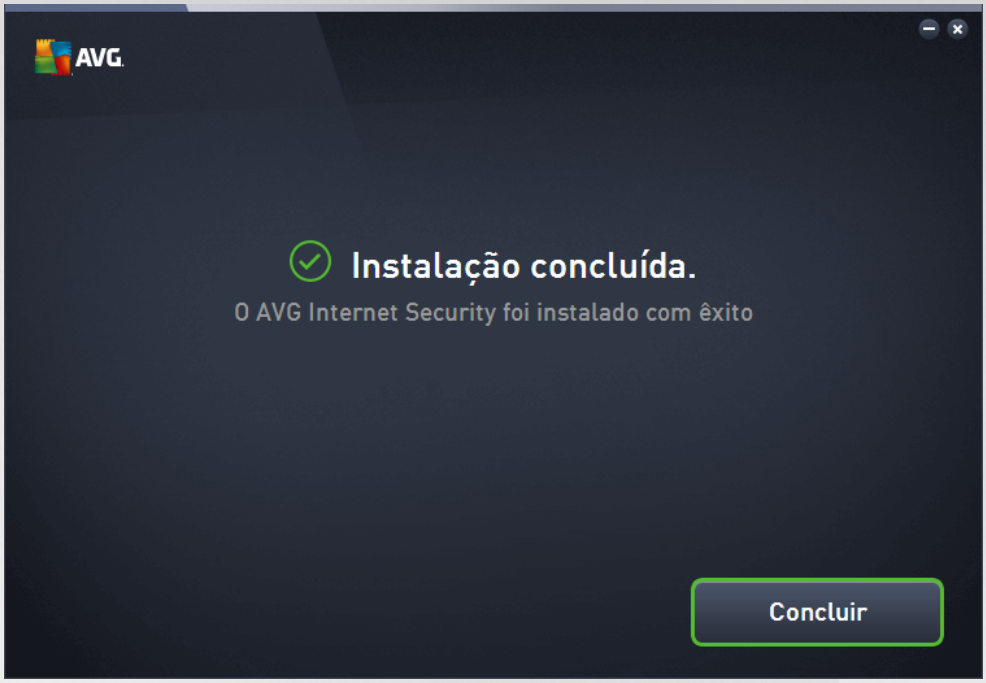
Botões de controlo

Existem dois botões de controlo disponíveis nesta janela:

- ***Minimizar*** – O processo de instalação poderá demorar vários minutos. Clique no botão para minimizar a janela para um ícone visível na barra do sistema. A janela aparece novamente quando a instalação estiver concluída.
- ***Cancelar*** – Este botão só deve ser usado se quiser parar o processo de instalação em curso. Tenha em conta que, nesse caso, o **AVG Internet Security** não será instalado!

3.5. Instalação concluída

A janela ***Parabéns*** confirma que o **AVG Internet Security** foi totalmente instalado e configurado:



Programa de Melhoria do Produto e Política de Privacidade

Aqui pode decidir se pretende participar no ***Programa de Melhoria do Produto*** (*para mais informações, consulte o capítulo Definições Avançadas do AVG / Programa de Melhoria do Produto*) que recolhe informações anónimas sobre as ameaças detetadas para aumentar o nível de segurança geral da Internet. Todos os dados são tratados como sendo confidenciais e em conformidade com a Política de Privacidade da AVG; clique na ligação ***Política de Privacidade*** para ser redirecionado para o website da AVG (http://www.avg.com/), onde poderá encontrar o texto integral da Política de Privacidade da AVG. Se aceitar, mantenha a opção assinalada *(a opção é confirmada por predefinição)*.

Para concluir o processo de instalação, clique no botão ***Terminar***.

4. Após a Instalação

4.1. Atualização da base de dados de vírus

Tenha em atenção que, após a instalação *(depois do reinício do computador, se for necessário)*, o **AVG Internet Security** atualiza automaticamente a base de dados de vírus e todos os componentes, deixando-os em perfeitas condições de funcionamento, o que pode demorar alguns minutos. Durante o processo de atualização, aparece informação relativa à operação na janela principal. Aguarde alguns momentos até o processo de atualização ficar concluído e terá o **AVG Internet Security** totalmente funcional e pronto para o proteger!

4.2. Registo do produto

Uma vez concluída a instalação do **AVG Internet Security**, registe o seu produto online no website da AVG (*http://www.avg.com/*). Após o registo terá acesso total à sua conta de utilizador AVG, ao boletim informativo de Atualização da AVG e a outros serviços fornecidos exclusivamente aos utilizadores registados. A forma mais fácil de fazer o registo é diretamente a partir da interface de utilizador do **AVG Internet Security**. Selecione o item navegação da linha superior / Opções / Registar agora. Será redirecionado para a página de ***Registo*** no website da AVG (*http://www.avg.com/*). Siga as instruções apresentadas na página.

4.3. Aceder à Interface de Utilizador

A janela principal do AVG pode ser acedida de muitas formas:

- fazendo duplo clique sobre o ícone do AVG na barra de tarefas
- fazendo duplo clique sobre o ícone do AVG no ambiente de trabalho
- a partir do menu ***Iniciar / Todos os Programas / AVG / AVG Protection***

4.4. Análise de todo o computador

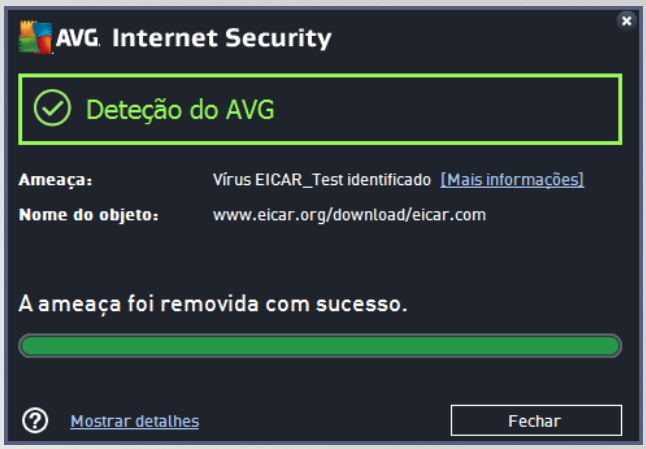
Existe um risco potencial de que um vírus informático tenha sido transmitido ao seu computador antes da instalação do **AVG Internet Security**. Por este motivo deve executar uma análise Analisar todo o computador para se certificar de que não existem infeções no seu PC. A primeira análise poderá demorar algum tempo *(cerca de uma hora)*, mas é aconselhável executar a análise para se certificar de que o seu computador não foi infetado por uma ameaça. Para instruções relativas à execução de Analisar todo o computador, consulte o capítulo Análise do AVG.

4.5. Teste Eicar

Para confirmar que o **AVG Internet Security** foi devidamente instalado, pode executar o teste EICAR.

O teste EICAR é um método padrão e absolutamente seguro concebido para testar o funcionamento de sistemas antivírus. Pode ser transmitido com segurança, uma vez que não é um vírus verdadeiro e não contém fragmentos de código de vírus. A maioria dos produtos reage como se tratasse de um vírus (*embora o refiram normalmente com um nome óbvio, tal como "EICAR-AV-Test"*). Pode transferir o vírus EICAR a partir do website da Eicar em www.eicar.com, onde poderá encontrar igualmente todas as informações necessárias sobre o teste.

Tente transferir o ficheiro *eicar.com* e guardá-lo no disco local. Imediatamente após a confirmação da transferência do ficheiro de teste, o **AVG Internet Security** reagirá ao ficheiro com um aviso. Esse aviso demonstra que o AVG está corretamente instalado no seu computador.



Se o AVG não identificar o ficheiro de teste EICAR como um vírus, verifique novamente a configuração do programa!

4.6. Configuração predefinida do AVG

A configuração predefinida (*ou seja, a forma como a aplicação está configurada imediatamente após a instalação*) do **AVG Internet Security** é definida pelo fornecedor do software de forma a que todos os componentes e funções estejam afinados para proporcionarem um desempenho excelente. ***Não altere a configuração do AVG a menos que tenha uma razão imperativa para o fazer. Quaisquer alterações às definições deverão ser efetuadas exclusivamente por um utilizador avançado.*** Se quiser alterar a configuração do AVG para esta corresponder melhor às suas necessidades, vá a Definições Avançadas do AVG: selecione o item do menu principal *Opções/Definições avançadas* e edite a configuração do AVG na janela Definições Avançadas do AVG apresentada.

5. Interface de Utilizador do AVG

O **AVG Internet Security** abre com a janela principal:

A janela principal está dividida em várias secções:

- A ***navegação da linha superior*** consiste em quatro ligações ativas alinhadas na parte superior da janela principal *(Gosta do AVG, Relatórios, Suporte, Opções)*. Detalhes >>
- A ***Informação de Estado de Segurança*** disponibiliza informação básica relativa ao estado atual do **AVG Internet Security**. Detalhes >>
- A ***síntese de componentes instalados*** encontra-se numa faixa horizontal de blocos na secção central da janela principal. Os componentes são apresentados sob a forma de blocos de cor verde claro, identificados pelo respetivo ícone de componente, sendo também apresentada a informação relativa ao estado do componente. Detalhes >>
- As ***Minhas Aplicações*** são apresentadas graficamente na faixa central inferior da janela principal e disponibilizam uma visão geral das aplicações complementares do **AVG Internet Security** que já estão instaladas no computador ou cuja instalação é recomendada. Detalhes >>
- Os ***links rápidos de Analisar / Corrigir / Atualizar*** encontram-se na linha inferior de blocos na janela principal. Estes botões permitem aceder de imediato às funções mais importantes e mais frequentes do AVG. Detalhes >>

Fora da janela principal do **AVG Internet Security**, existe mais um elemento de controlo que poderá utilizar para aceder à aplicação:

- O ***ícone da barra de tarefas*** encontra-se no canto inferior direito do monitor *(na barra de tarefas)* e indica o estado atual do **AVG Internet Security**. Detalhes >>

5.1. Navegação da Linha Superior

A ***navegação da linha superior*** consiste em várias ligações ativas alinhadas na parte superior da janela principal. A navegação inclui os seguintes botões:

5.1.1. Junte-se a nós no Facebook

Clique uma vez na ligação para se ligar à comunidade AVG no Facebook e partilhar as mais recentes informações, novidades, dicas e sugestões do AVG para obter segurança máxima na Internet.

5.1.2. Relatórios

Abre uma nova janela de ***Relatórios*** com uma síntese de todos os relatórios relevantes referentes a análises e processos de atualização iniciados anteriormente. Se a análise ou atualização estiver em execução, é apresentado um círculo em rotação junto ao texto ***Relatórios*** na navegação superior da interface de utilizador principal. Clique nesse círculo para aceder à janela de visualização do progresso do processo em execução:

5.1.3. Suporte

Abre uma nova janela dividida em quatro separadores, onde pode encontrar todas as informações relevantes sobre o **AVG Internet Security**:

AVG Internet Security
Licença e suporte
Produto
Programa
Contrato de Licença
Informações da licença
Nome do produto: AVG Internet Security (Completo, 1 posto)
Número de Licença: I073H-JDFB6-6G7JM-QUM3E-9L7G2-N (copiar para a área de transferência)
Licença Expira: Wednesday, December 28, 2050 Renovar agora
Comprou uma nova licença?
Reativar
Support information
Contact Support
Get the answers you need from our experts.
CONTACT SUPPORT
AVG Community
Give advice. Get advice. Share knowledge in our free community.
LEARN & SHARE
FAQs
Find answers to Frequently Asked Questions on our website.
VISIT FAQS
Virus removal tools
Remove viruses and infections with our free virus removal tools.
GET VIRUS REMOVALS
Fechar

- ***Licença e suporte*** – Este separador apresenta informações relativas ao nome do produto, ao número de licença e à data de expiração. Na parte inferior da janela também pode encontrar uma síntese organizada de todos os contactos disponíveis para apoio ao cliente. Estão disponíveis no separador as seguintes ligações ativas e os seguintes botões:

    - *(Re)ativar* – Clique para abrir a nova janela de ***Ativar Software AVG***. Preencha o seu número de licença no campo respetivo para substituir o número de venda *(utilizado durante a instalação do AVG Internet Security)* ou para substituir o número de licença atual por outro *(por exemplo, ao atualizar para um produto AVG superior)*..

    - *Copiar para a área de transferência* – Utilize esta ligação para copiar o número de licença e colá-lo onde for necessário. Dessa forma pode certificar-se de que o número é introduzido corretamente.

    - *Renovar agora* – Recomendamos que adquira a renovação de licença do **AVG Internet Security** atempadamente, pelo menos um mês antes da expiração da licença atual. Será informado quando a data de expiração estiver próxima. Clique nesta ligação para ser redirecionado para o website da AVG *(http://www.avg.com/)*, onde pode encontrar informações detalhadas relativas ao estado da licença, à data de expiração e à oferta de renovação/ atualização.

- ***Produto*** – Este separador apresenta uma síntese dos dados técnicos mais importantes do **AVG Internet Security** no que diz respeito a informações do produto, componentes instalados e proteção de e-mail instalada.

- ***Programa*** – Neste separador pode encontrar informações relativas à versão do ficheiro do programa e a código de terceiros utilizado no produto.

- ***Contrato de Licença*** – Este separador apresenta o texto integral do contrato de licença entre o utilizador e a AVG Technologies.

5.1.4. Opções

É possível aceder à manutenção do **AVG Internet Security** através do item ***Opções***. Clique na seta para abrir o menu pendente:

- ***Analisar o computador*** – Inicia uma análise de todo o computador.
- ***Analisar pasta selecionada...*** – Muda para a interface de análise do AVG e permite-lhe definir na estrutura em árvore do seu computador quais os ficheiros e pastas que devem ser analisados.
- ***Analisar ficheiro...*** – Permite-lhe executar um teste manual de um ficheiro específico. Clique nesta opção para abrir uma nova janela com a estrutura em árvore do disco. Selecione o ficheiro pretendido e confirme o início da análise.
- ***Atualizar*** – Inicia automaticamente o processo de atualização do **AVG Internet Security**.
- ***Atualizar a partir do diretório...*** – Executa o processo de atualização a partir dos ficheiros de atualização localizados numa pasta específica no seu disco local. No entanto, esta opção só é recomendada como emergência, ex. em situações em que não está disponível uma ligação à Internet (por exemplo, o seu computador está infetado e desligado da Internet, o seu computador está ligado a uma rede sem acesso à Internet, etc.). Na nova janela, selecione a pasta na qual colocou anteriormente o ficheiro de atualização e inicie o processo de atualização.
- ***Quarentena de Vírus*** – Abre a interface do espaço de quarentena, a Quarentena de Vírus, para onde o AVG remove todas as infeções detetadas. Nesta quarentena, os ficheiros infetados são isolados e a segurança do seu computador está assegurada, enquanto que os ficheiros infetados são armazenados para possíveis reparações futuras.
- ***Histórico*** – Disponibiliza opções adicionais de submenus específicos:
  - *Resultados da Análise* – Abre uma janela que apresenta um resumo dos resultados da análise.
  - *Resultados da Proteção Residente* – Abre uma janela com uma síntese das ameaças detetadas pela Proteção Residente.
  - *Resultados da Proteção de Identidade* – Abre uma janela com uma síntese das ameaças detetadas pelo componente Identidade.
  - *Resultados da Proteção de E-mail* – Abre uma janela com uma síntese dos anexos de mensagens de e-mail identificados como perigosos pelo componente Proteção de E-mail.
  - *Resultados da Proteção Online* – Abre uma janela com uma síntese das ameaças detetadas pela Proteção Online.
  - *Registo do Histórico de Eventos* – Abre a interface de registo do histórico com uma síntese de todas as ações do **AVG Internet Security** registadas.
  - *Registo da Firewall* – Abre uma janela com uma síntese detalhada de todas as ações da Firewall.

- ***Definições avançadas...*** – Abre a janela de definições avançadas do AVG, na qual pode editar a configuração do **AVG Internet Security**. Regra geral, é recomendável manter as predefinições da aplicação conforme definidas pelo fornecedor do software.

- ***Definições da Firewall...*** – Abre uma janela independente para configuração avançada do componente Firewall.

- ***Conteúdos de ajuda*** – Abre os ficheiros de ajuda do AVG.

- ***Obter suporte*** – Abre a janela de suporte que disponibiliza todos os contactos acessíveis e informações de suporte.

- ***A sua Internet AVG*** – Abre o website da AVG (*http://www.avg.com/*).

- ***Acerca de Vírus e Ameaças*** – Abre a enciclopédia de vírus online no website da AVG (*http://www.avg.com/*), onde pode consultar informações detalhadas sobre o vírus identificado.

- ***(Re)Ativar*** – Abre a janela de ativação com o número de licença que disponibilizou durante o processo de instalação. Nessa janela pode editar o seu número de licença para substituir o número de venda (*com o qual instalou o AVG*) ou para substituir o número de licença antigo (*por exemplo, ao atualizar para um novo produto AVG*). Se estiver a utilizar a versão de teste do **AVG Internet Security**, os dois últimos itens aparecem como ***Comprar agora*** e ***Ativar***, permitindo-lhe comprar a versão completa do programa imediatamente. No caso de um produto **AVG Internet Security** instalado com um número de venda, os itens são apresentados como ***Registar*** e ***Ativar***:

- ***Registar agora / MyAccount*** – Faz a ligação à página de registo do site da AVG (*http://www.avg.com/*). Por favor preencha os seus dados de registo; somente os clientes que registem o seu produto AVG podem receber suporte técnico gratuito.

- ***Acerca do AVG*** – Abre uma nova janela com quatro separadores que apresentam os dados relativos à licença adquirida e ao suporte acessível, informações relativas aos produtos e ao programa e o texto completo do contrato de licença. *(É possível abrir essa mesma janela através da ligação Suporte da navegação principal.)*

5.2. Informação de Estado de Segurança

A secção ***Informação de Estado de Segurança*** está localizada na parte superior da janela principal do **AVG Internet Security**. Nesta secção encontra sempre informações relativas ao estado de segurança atual do **AVG Internet Security**. Veja uma síntese dos ícones possivelmente apresentados e a respetiva descrição:

– o ícone verde indica que o ***AVG Internet Security está completamente funcional***. O computador está totalmente protegido, atualizado e todos os componentes instalados estão a funcionar corretamente.

– o ícone amarelo avisa que ***um ou mais componentes não estão configurados corretamente***, devendo o utilizador verificar as respetivas propriedades/definições. Não existem problemas críticos no **AVG Internet Security** e provavelmente decidiu desativar um componente por alguma razão. Ainda continua protegido! No entanto, preste atenção às definições do componente problemático! O componente configurado incorretamente será apresentado com uma faixa de aviso cor de laranja na interface de utilizador principal.

O ícone amarelo também é apresentado se, por alguma razão, tiver decidido ignorar o estado de erro de um componente. Pode aceder à opção ***Ignorar estado de erro*** no separador Definições avançadas / Ignorar estado de erro. Aí terá a opção de indicar que está ciente do estado de erro do componente, mas que por alguma razão pretende manter o **AVG Internet Security** nesse estado e não pretende ser avisado. Poderá ser necessário utilizar esta opção numa situação específica, mas é especialmente recomendado desativar a opção ***Ignorar estado de erro*** o mais rapidamente possível!

Em alternativa, o ícone amarelo também é apresentado se o **AVG Internet Security** necessitar do reinício do computador (***Reinício necessário***). Preste especial atenção a esse aviso e reinicie o computador.

– o ícone cor de laranja indica que o ***AVG Internet Security está em estado crítico***! Um ou mais componentes não funcionam devidamente e o **AVG Internet Security** não consegue proteger o computador. Preste atenção imediata à resolução do problema referenciado! Se não conseguir resolver o problema sozinho, contacte a equipa de suporte técnico da AVG.

Na eventualidade de o AVG Internet Security não estar configurado para o melhor desempenho, há um novo botão Clique para corrigir (ou Clique para corrigir tudo, se o problema envolver mais de um componente) que aparece junto à informação do estado de segurança. Clique no botão para iniciar um processo automático de verificação e configuração do programa. É uma forma fácil de configurar o AVG Internet Security para um desempenho otimizado e obter o nível máximo de segurança!

É recomendável que preste atenção à ***Informação de Estado de Segurança*** e se o relatório indicar algum problema, tente resolvê-lo imediatamente. Caso contrário, o seu computador está em risco!

Nota: *a informação relativa ao estado do AVG Internet Security também pode ser obtida a qualquer altura a partir do ícone da barra de tarefas.*

5.3. Síntese de Componentes

A ***síntese de componentes instalados*** encontra-se numa faixa horizontal de blocos na secção central da janela principal. Os componentes são apresentados sob a forma de blocos de cor verde claro, identificados pelo respetivo ícone de componente. Cada bloco apresenta informação relativa ao estado atual de proteção. Se o componente estiver configurado corretamente e totalmente funcional, a informação aparece com letras verdes. Se o componente for desativado, se a funcionalidade ficar limitada ou se o componente estiver em estado de erro, o utilizador será notificado através de um texto de aviso apresentado num campo de texto cor de laranja. ***Recomendamos veementemente que preste atenção às definições do componente respetivo!***

Desloque o rato sobre o componente para ver um pequeno texto na parte inferior da janela principal. O texto disponibiliza uma introdução básica à funcionalidade do componente. Além disso, apresenta informação relativa ao estado atual do componente e indica qual dos serviços do componente não está configurado corretamente.

Lista de componentes instalados

No **AVG Internet Security**, a secção ***Síntese de Componentes*** contém informações relativas aos seguintes componentes:

- ***Computador*** – Este componente abrange dois serviços: a ***Proteção Antivírus*** deteta vírus, spyware, worms, cavalos de Troia, ficheiros executáveis indesejados ou bibliotecas dentro do seu sistema e

protege-o de adware malicioso; o serviço ***Anti-Rootkit*** analisa o computador em busca de rootkits perigosos escondidos dentro de aplicações, controladores ou bibliotecas. Detalhes >>

- ***Web*** – Protege-o contra ataques com base na Internet enquanto pesquisa e navega na Internet. Detalhes >>
- ***Identidade*** – Este componente executa o serviço ***Proteção de Identidade***, que protege continuamente os seus recursos digitais contra ameaças novas e desconhecidas existentes na Internet. Detalhes >>
- ***E-mails*** – Verifica as mensagens de correio de entrada pela existência de SPAM e bloqueia vírus, ataques de phishing ou outras ameaças. Detalhes >>
- ***Firewall*** – Controla todas as comunicações em todas as portas de rede, protegendo-o contra ataques maliciosos e bloqueando todas as tentativas de intrusão. Detalhes >>

Ações acessíveis

- ***Coloque o rato sobre o ícone de qualquer componente*** para o realçar na síntese de componentes. É apresentada simultaneamente uma descrição da funcionalidade básica do componente na parte inferior da interface de utilizador.
- ***Clique uma vez no ícone do componente*** para abrir a interface específica do mesmo, que inclui informação relativa ao estado atual do componente e acesso à configuração e aos dados estatísticos do componente.

5.4. As Minhas Aplicações

Na área ***As Minhas Aplicações*** *(a linha de blocos verdes por baixo do conjunto de componentes)* pode encontrar uma síntese de aplicações AVG adicionais que já estão instaladas no computador ou cuja instalação é recomendada. Os blocos apresentados variam e poderão representar qualquer uma das seguintes aplicações:

- ***Proteção móvel*** é uma aplicação que protege o seu telemóvel contra vírus e malware. Disponibiliza também a capacidade de localizar o seu smartphone remotamente se ficar separado do mesmo.
- A aplicação ***LiveKive*** destina-se à cópia de segurança online de dados em servidores seguros. O LiveKive faz cópias de segurança automáticas de todos os seus ficheiros, fotografias e músicas para um local seguro, permitindo que os partilhe com os seus familiares e amigos e aceda aos mesmos a partir de qualquer dispositivo com ligação à Internet, incluindo dispositivos iPhone e Android.
- A aplicação ***Family Safety*** ajuda-o a proteger os seus filhos de websites, conteúdos multimédia e pesquisas online inapropriados, proporcionando-lhe relatórios relativos à atividade deles online. O AVG Family Safety utiliza tecnologia de pressão de teclas para monitorizar as atividades do seu filho em salas de chat e em sites de redes sociais. Se a aplicação detetar palavras, expressões ou linguagem conhecidas por serem utilizadas para vitimizar crianças online, receberá de imediato uma notificação através de SMS ou e-mail. A aplicação permite-lhe definir o nível de proteção adequado para cada um dos seus filhos e monitorizá-los separadamente por meio de credenciais de início de sessão individuais.
- A aplicação ***PC TuneUp*** é uma ferramenta avançada que permite analisar e corrigir o sistema

detalhadamente de modo a melhorar a velocidade e o desempenho geral do computador.

- A ***AVG Toolbar*** está disponível diretamente no seu browser de Internet e garante segurança máxima durante a navegação na Internet.

Para obter informações detalhadas sobre qualquer uma das aplicações incluídas em ***As Minhas Aplicações***, clique no bloco respetivo. Será redirecionado para a página dedicada do AVG, onde poderá também transferir o componente de imediato.

5.5. Links Rápidos de Analisar/Atualizar

Os ***links rápidos*** encontram-se na linha inferior de botões localizados na interface de utilizador do **AVG Internet Security**. Estes links permitem-lhe aceder imediatamente às funcionalidades mais importantes e mais frequentemente usadas da aplicação, ou seja, as análises e as atualizações. Os links rápidos são acessíveis a partir de qualquer janela da interface de utilizador:

- ***Analisar agora*** – O botão está dividido graficamente em duas secções. Clique no link ***Analisar agora*** para iniciar de imediato a operação Analisar todo o computador e veja o progresso e os resultados na janela Relatórios que é aberta automaticamente. O botão ***Opções*** abre a janela ***Opções de análise***, na qual pode gerir análises agendadas e editar parâmetros de Analisar todo o computador / Analisar pastas ou ficheiros. *(Para mais informações, consulte o capítulo Análise do AVG)*

- ***Corrigir desempenho*** – O botão permite aceder ao serviço ***Analisador do PC***, uma ferramenta avançada que permite analisar e corrigir o sistema detalhadamente de modo a melhorar a velocidade e o desempenho geral do computador.

- ***Atualizar agora*** – Clique no botão para iniciar de imediato a atualização do produto. Será informado dos resultados da atualização na janela deslizante que aparece por cima do ícone do AVG na barra de tarefas. *(Para mais informações, consulte o capítulo Atualizações do AVG)*

5.6. Ícone da barra de tarefas

O ***ícone do AVG na barra de tarefas*** *(na barra de tarefas do Windows, canto inferior direito do ecrã)* indica o estado atual do **AVG Internet Security**. Está constantemente visível na barra de tarefas, independentemente de a interface de utilizador do **AVG Internet Security** estar aberta ou fechada:

Apresentação do Ícone do AVG na Barra de Tarefas

- Com cor cheia, sem elementos adicionais, o ícone indica que todos os componentes do **AVG**

Internet Security estão ativos e perfeitamente funcionais. No entanto, o ícone também pode ser apresentado desta forma numa situação em que um dos componentes não esteja completamente funcional, mas o utilizador tenha decidido ignorar o estado do componente. *(Tendo confirmado a opção de ignorar o estado do componente, exprime que está ciente do estado de erro do componente, mas que, por alguma razão, pretende mantê-lo assim e não quer ser notificado sobre essa situação.)*

- O ícone com um ponto de exclamação indica que um componente *(ou vários componentes)* está em estado de erro. Preste sempre atenção a este aviso e tente corrigir o problema de configuração no caso de um componente que não esteja configurado corretamente. Para poder efetuar as alterações necessárias à configuração do componente, clique duas vezes no ícone da barra de tarefas para abrir a interface de utilizador da aplicação. Para informações detalhadas sobre os componentes que estão em estado de erro, consulte a secção de informação de estado de segurança.

- O ícone da barra de tarefas pode ainda ser apresentado com cor cheia e com um raio de luz rotativo e intermitente. Essa versão gráfica indica um processo de atualização em curso.

- A apresentação alternativa de um ícone com cor cheia e uma seta indica que uma das análises do **AVG Internet Security** está em execução.

Informações do Ícone do AVG na Barra de Tarefas

O ***ícone do AVG na barra de tarefas*** informa também sobre as atividades do **AVG Internet Security** e possíveis alterações de estado no programa (*por exemplo, início automático de uma análise ou atualização agendada, mudança de perfil da Firewall, alteração de estado de um componente, ocorrência de estado de erro, etc.*) por meio de uma janela pop-up aberta a partir do ícone da barra de tarefas.

Ações acessíveis a partir do Ícone do AVG na Barra de Tarefas

O ***ícone do AVG na barra de tarefas*** também pode ser utilizado como ligação rápida para aceder à interface de utilizador do **AVG Internet Security**; basta clicar duas vezes no ícone. Ao clicar com o botão direito do rato no ícone abre um pequeno menu de contexto com as seguintes opções:

- ***Abrir AVG*** – clique para abrir a interface de utilizador do **AVG Internet Security**.

- ***Desativar temporariamente a proteção do AVG*** – esta opção permite-lhe desativar toda a proteção assegurada pelo **AVG Internet Security** de uma só vez. Tenha em atenção que não deverá usar esta opção a menos que seja absolutamente necessário! Na maioria dos casos, não é necessário desativar o **AVG Internet Security** antes de instalar novo software ou controladores, mesmo que o instalador ou o assistente do software sugiram que os programas e aplicações em execução devam ser encerrados primeiro para garantir que não ocorrem interrupções durante o processo de instalação. Se tiver de desativar o **AVG Internet Security** temporariamente, deverá voltar a ativá-lo assim que terminar. Se estiver ligado à Internet ou a uma rede durante o período de desativação do software antivírus, o seu computador estará vulnerável a ataques.

- ***Analisar*** – clique para abrir o menu de contexto das análises predefinidas (*Analisar todo o computador* e *Analisar pastas ou ficheiros*) e selecione a análise pretendida; a análise será iniciada imediatamente.

- ***Firewall*** – clique para abrir o menu de contexto com acesso rápido a todos os modos da Firewall disponíveis. Selecione uma opção na visão geral e clique para confirmar que pretende alterar o modo da Firewall que está configurado.

- ***Análises em execução...*** – este item só é apresentado se houver uma análise em execução no computador. É possível definir a prioridade desta análise, parar ou pausar a análise. Também é possível aceder às seguintes ações: *Definir prioridade para todas as análises, Pausar todas as análises* ou *Parar todas as análises*.

- ***Corrigir desempenho*** – clique para iniciar o componente Analisador do PC.

- ***Iniciar sessão em AVG MyAccount*** – abre a página inicial de MyAccount, na qual pode gerir as subscrições dos seus produtos, adquirir proteção adicional, transferir ficheiros de instalação, verificar encomendas e faturas anteriores, e gerir os seus dados pessoais.

- ***Atualizar agora*** – inicia imediatamente uma atualização.

- ***Ajuda*** – abre o ficheiro de ajuda na página inicial.

5.7. Conselho do AVG

O ***Conselho do AVG*** foi concebido para detetar problemas que poderão estar a tornar o computador mais lento ou a colocá-lo em risco e, posteriormente, recomendar uma ação para resolver o problema. Quando um computador fica subitamente mais lento *(navegação na Internet, desempenho geral)*, normalmente não é fácil identificar de imediato o que está a causar essa lentidão e o que será necessário fazer para resolver o problema. É essa a função do ***Conselho do AVG***: este componente apresenta uma notificação na barra de tarefas a informar o utilizador de qual poderá ser o problema e sugere uma forma de o resolver. O ***Conselho do AVG*** monitoriza continuamente todos os processos em execução no computador em busca de possíveis problemas, apresentando dicas para evitar esses problemas.

O ***Conselho do AVG*** aparece sob a forma de uma janela pop-up por cima da barra de tarefas:

AVG Internet Security
Elevada utilização de memória detetada
Internet Explorer
Memória utilizada: 941 MB
O AVG recomenda fechar e voltar a abrir a aplicação para obter melhor desempenho.
Opções de notificação

O ***Conselho do AVG*** monitoriza especificamente o seguinte:

- ***O estado de qualquer browser que esteja aberto***. Os browsers podem sobrecarregar a memória, particularmente se vários separadores ou várias janelas estiverem abertos há algum tempo, e utilizam uma grande quantidade dos recursos do sistema, ou seja, tornam o computador mais lento. Nesse caso, reiniciar o browser ajuda normalmente a resolver o problema.

- ***Ligações Ponto-a-Ponto (P2P) em execução***. Após a utilização do protocolo P2P para partilhar ficheiros, a ligação poderá permanecer ativa, utilizando uma determinada quantidade da largura de banda. Consequentemente, a navegação na Internet poderá ficar mais lenta.

- ***Rede desconhecida com um nome familiar***. Esta situação normalmente aplica-se apenas a utilizadores que estabelecem ligação a várias redes, usualmente com computadores portáteis: se uma rede nova e desconhecida tiver o mesmo nome de uma rede conhecida e utilizada com frequência *(por exemplo, Casa ou A minha Wi-Fi)*, poderá existir alguma confusão e poderá ser estabelecida uma ligação acidentalmente a uma rede totalmente desconhecida e possivelmente perigosa. O ***Conselho do AVG*** pode evitar que isso aconteça avisando o utilizador de que o nome conhecido refere-se, na verdade, a uma nova rede. Obviamente, se o utilizador decidir que a rede desconhecida é segura, pode guardá-la numa lista de redes conhecidas do ***Conselho do AVG*** para que não seja reportada de futuro.

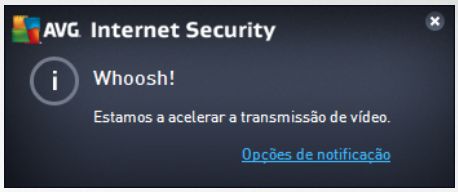
Em cada uma dessas situações, o ***Conselho do AVG*** avisa o utilizador relativamente ao problema que pode ocorrer e apresenta o nome e o ícone do processo ou da aplicação em conflito. O ***Conselho do AVG*** sugere também os passos que devem ser efetuados para evitar o problema.

Browsers suportados

Esta funcionalidade pode ser utilizada com os seguintes browsers: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.8. Acelerador AVG

O ***Acelerador AVG*** permite uma reprodução de vídeos online mais fluida e facilita as transferências. Quando o processo de aceleração do vídeo estiver em curso, será notificado via uma janela de notificação na barra de tarefas.



6. Componentes do AVG

6.1. Proteção do computador

O componente ***Computador*** abrange dois serviços de segurança principais: ***Antivírus*** e ***Cofre de Dados***:

- ***O serviço Antivírus*** consiste num componente de análise que protege todos os ficheiros, as áreas de sistema do computador e suportes amovíveis *(disco flash, etc.)* e executa análises para procurar vírus conhecidos. Quaisquer vírus detetados serão impedidos de tomarem qualquer ação e serão eliminados ou colocados na Quarentena de Vírus. O utilizador nem se apercebe do processo, uma vez que a chamada proteção residente trabalha "em segundo plano". O Antivírus também utiliza análise heurística, ou seja, os ficheiros são analisados para procurar características habituais de vírus. Isso significa que o Antivírus consegue detetar um novo vírus desconhecido se o vírus tiver algumas das características habituais dos vírus existentes. O **AVG Internet Security** também consegue analisar e detetar aplicações executáveis ou bibliotecas DLL que podem ser indesejadas no sistema *(diferentes tipos de spyware, adware, etc.)*. Adicionalmente, o Antivírus analisa o registo do sistema para verificar a existência de entradas suspeitas e ficheiros temporários da Internet, permitindo tratar todos os itens potencialmente indesejados da mesma forma que qualquer outra infeção.

- O serviço ***Cofre de Dados*** permite criar cofres virtuais seguros para guardar dados importantes ou sensíveis. O conteúdo de um Cofre de Dados é encriptado e protegido por meio de uma palavra-passe à sua escolha, para que ninguém possa aceder ao cofre sem autorização.

AVG Internet Security
Proteção do computador
Antivírus
ATIVADO
Cofre de Dados
COMECE A UTILIZAR O COFRE
CRIAR COFRE
Proteção em tempo real contra vírus, spyware, cavalos de Troia e outros tipos de malware.
Encripte e proteja qualquer ficheiro por palavra-passe para evitar espionagem.
compilação 7132

Controlos da janela

Para alternar entre as duas secções da janela, pode simplesmente clicar em qualquer parte do painel do serviço respetivo. O painel fica realçado com um tom de azul mais claro. Pode encontrar os controlos que se seguem nas duas secções da janela. A funcionalidade dos controlos é igual independentemente do serviço de segurança a que pertençam *(Antivírus ou Cofre de Dados)*:

Ativado / Desativado – O botão poderá fazer lembrar as luzes de um semáforo, tanto no aspeto como na funcionalidade. Clique uma vez para alternar entre as duas posições. A cor verde indica o estado ***Ativado***, que significa que o serviço de segurança Antivírus está ativo e totalmente funcional. A cor vermelha representa o estado ***Desativado***, ou seja, o serviço está desativado. Se não tiver um motivo aceitável para desativar o serviço, recomendamos que mantenha as predefinições de toda a configuração de segurança. As predefinições asseguram o desempenho ideal da aplicação e a segurança máxima do utilizador. Se por algum motivo pretender desativar o serviço, será avisado imediatamente da possibilidade de risco através da indicação ***Aviso*** a vermelho e da informação de que não se encontra totalmente protegido de momento. ***Tenha em atenção que deverá reativar o serviço o mais rapidamente possível!***

Definições – Clique no botão para ser redirecionado para a interface de definições avançadas. A janela respetiva é aberta e poderá configurar o serviço selecionado, ou seja, o Antivírus. Na interface de definições avançadas pode editar toda a configuração de cada serviço de segurança do **AVG Internet Security**, mas qualquer configuração deve ser efetuada apenas por utilizadores experientes!

Seta – Utilize a seta verde na parte superior esquerda da janela para voltar à interface de utilizador principal com a síntese dos componentes.

Como criar um cofre de dados

Na secção ***Cofre de Dados*** da janela ***Proteção do computador*** pode encontrar o botão ***Criar um Cofre***. Clique no botão para abrir uma nova janela com o mesmo nome, na qual pode especificar os parâmetros do cofre pretendido. Preencha todas as informações necessárias e siga as instruções apresentadas na aplicação:

Em primeiro lugar, é necessário especificar o nome do cofre e criar uma palavra-passe forte:

- ***Nome do Cofre*** – Para criar um novo cofre de dados, é necessário escolher primeiro um nome adequado para conseguir reconhecer o cofre. Se partilhar o computador com familiares, poderá também incluir o seu nome e uma indicação do conteúdo do cofre, por exemplo, *E-mails do pai*.

- ***Criar palavra-passe / Voltar a digitar palavra-passe*** – Crie uma palavra-passe para o cofre de dados e introduza-a nos campos de texto respetivos. O indicador gráfico no lado direito dir-lhe-á se a palavra-passe escolhida é fraca *(relativamente fácil de decifrar com ferramentas especiais de software)* ou forte. É aconselhável escolher uma palavra-passe que tenha no mínimo uma força média. Pode tornar a sua palavra-passe mais forte incluindo letras maiúsculas, números e outros caracteres como, por exemplo, pontos, traços, etc. Se quiser certificar-se de que digita a palavra-passe conforme pretendido, pode marcar a caixa ***Mostrar palavra-passe*** *(obviamente, mais ninguém deverá estar a olhar para o seu ecrã).*.

- ***Dica de palavra-passe*** – É extremamente aconselhável criar também uma dica de palavra-passe útil que o ajude a lembrar-se da sua palavra-passe no caso de se esquecer da mesma. Lembre-se de que um Cofre de Dados é concebido para manter os seus ficheiros protegidos permitindo o acesso apenas através de palavra-passe; não existem métodos de acesso alternativos. Se se esquecer da palavra-passe, não poderá aceder ao seu cofre de dados!

Depois de especificar todos os dados necessários nos campos de texto, clique no botão ***Seguinte*** para avançar para o passo seguinte:

AVG Internet Security
Criar Novo Cofre de Dados - My private documents
Selecione a localização e o tamanho do cofre.
Localização:
C:\Users\Administrator\Documents
Procurar
Tamanho:
200 MB
(disponível: 2 GB)
Não sabe ao certo de que tamanho precisa? Selecione uma pasta com os ficheiros que pretende adicionar ao cofre para obter uma estimativa.
Acesso:
Criar atalho no ambiente de trabalho
Adicionar aos favoritos no Explorador do Windows
O cofre será guardado na localização selecionada como: My private documents.
Para abrir o cofre, basta clicar duas vezes no mesmo, como qualquer outro ficheiro.
Criar Cofre
compilação 7132

Esta janela disponibiliza as seguintes opções de configuração:

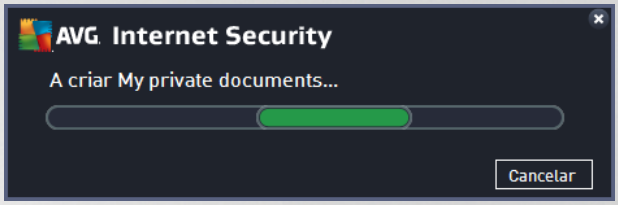
- ***Localização*** indica a localização física na qual será colocado o cofre de dados. Procure um destino adequado no disco rígido ou pode manter a localização predefinida, que é a pasta *Documentos*. Tenha em atenção que, uma vez criado um cofre de dados, não é possível alterar a sua localização.

- ***Tamanho*** – pode pré-configurar o tamanho do cofre de dados, que irá atribuir o espaço necessário no disco. O valor definido não deve ser nem muito pequeno *(insuficiente para as suas necessidades)*, nem muito grande *(ocupar demasiado espaço no disco desnecessariamente)*. Se já souber o que pretende guardar no cofre de dados, pode colocar todos os ficheiros numa pasta e utilizar a ligação ***Selecione uma pasta*** para calcular automaticamente o tamanho total. No entanto, pode alterar o tamanho posteriormente consoante as suas necessidades.

- ***Acesso*** – as caixas de verificação nesta secção permitem criar atalhos convenientes para aceder ao cofre de dados.

Como utilizar o cofre de dados

Quando estiver satisfeito com as definições, clique no botão ***Criar Cofre***. Aparece uma nova caixa de diálogo com o título ***O Cofre de Dados já está pronto*** a indicar que o cofre está disponível para armazenamento de ficheiros. Nesse momento, o cofre está aberto e é possível aceder de imediato ao mesmo. Sempre que tentar aceder ao cofre posteriormente, ser-lhe-á solicitado que desbloqueie o cofre com a palavra-passe definida:



Para utilizar o novo cofre de dados, é necessário abri-lo primeiro – clique no botão ***Abrir agora***. Depois de o abrir, o cofre de dados aparece no computador como um novo disco virtual. Atribua ao disco uma letra à sua escolha selecionada no menu pendente (*só poderá selecionar uma letra de entre os discos que estão livres*). Normalmente, não poderá escolher a letra C *(atribuída habitualmente ao disco rígido)*, a letra A *(unidade de disquete)* ou a letra D *(unidade de DVD)*. Tenha em atenção que, sempre que desbloqueia um cofre de dados, pode selecionar uma letra de unidade diferente que esteja disponível.

Como desbloquear o cofre de dados

Quando tentar aceder ao cofre de dados posteriormente, ser-lhe-á solicitado que desbloqueie o cofre com a palavra-passe definida:

No campo de texto, digite a palavra-passe para conceder autorização a si mesmo e clique no botão ***Desbloquear***. Se precisar de ajuda para se lembrar da palavra-passe, clique em ***Dica*** para ver a dica de palavra-passe que definiu aquando da criação do cofre de dados. O novo cofre de dados irá aparecer na síntese dos seus cofres de dados com a indicação DESBLOQUEADO e poderá adicionar/remover ficheiros do cofre conforme necessário.

6.2. Proteção de navegação na Web

A ***Proteção de navegação na Web*** consiste em dois serviços: ***LinkScanner Surf-Shield*** e ***Proteção Online***:

- ***O LinkScanner Surf-Shield*** protege-o contra o crescente número de ameaças 'transitórias' que populam a Internet. Estas ameaças podem estar ocultas em qualquer tipo de website, desde websites governamentais a websites de grandes multinacionais ou de pequenas empresas, e raramente permanecem nesses sites por mais de 24 horas. O LinkScanner protege-o ao analisar as páginas Web associadas a todos os links em qualquer página que esteja a visualizar e ao assegurar que estas são seguras no único momento em que importa – quando o utilizador está prestes a clicar no link. ***O LinkScanner Surf-Shield não se destina à proteção de plataformas de servidores!***

- ***A Proteção Online*** é um tipo de proteção residente em tempo real; analisa o conteúdo da páginas Web visitadas (e possíveis ficheiros incluídos nestas) mesmo antes destas serem apresentadas no seu browser ou serem transferidas para o seu computador. A Proteção Online deteta que a página que está prestes a visitar inclui algum javascript perigoso e evita que a página seja apresentada. Além disso, reconhece malware contido na página e interrompe a sua transferência imediatamente para que este nunca aceda ao seu computador. Esta poderosa proteção bloqueará o conteúdo malicioso de qualquer página Web que tentar abrir e evita que o mesmo seja transferido para o seu computador. Com esta funcionalidade ativada, clicar num link ou digitar um URL de um sítio perigoso bloqueará automaticamente a abertura da página Web, protegendo-o de ser inadvertidamente infetado. É importante lembrar que as páginas Web comprometidas podem infetar o seu computador através de uma simples visita ao site afetado. ***A Proteção Online não se destina a plataformas de servidores!***

Controlos da janela

Para alternar entre as duas secções da janela, pode simplesmente clicar em qualquer parte do painel do serviço respetivo. O painel fica realçado com um tom de azul mais claro. Pode encontrar os controlos que se seguem nas duas secções da janela. A funcionalidade dos controlos é igual independentemente do serviço de segurança a que pertençam *(LinkScanner Surf-Shield ou Proteção Online)*:

Ativado / Desativado – O botão poderá fazer lembrar as luzes de um semáforo, tanto no aspeto como na funcionalidade. Clique uma vez para alternar entre as duas posições. A cor verde indica o estado ***Ativado***, que significa que o serviço de segurança LinkScanner Surf-Shield / Proteção Online está ativo e totalmente funcional. A cor vermelha representa o estado ***Desativado***, ou seja, o serviço está desativado. Se não tiver um motivo aceitável para desativar o serviço, recomendamos que mantenha as predefinições de toda a configuração de segurança. As predefinições asseguram o desempenho ideal da aplicação e a segurança máxima do utilizador. Se por algum motivo pretender desativar o serviço, será avisado imediatamente da possibilidade de risco através da indicação ***Aviso*** a vermelho e da informação de que não se encontra totalmente protegido de momento. ***Tenha em atenção que deverá reativar o serviço o mais rapidamente possível!***

Definições – Clique no botão para ser redirecionado para a interface de definições avançadas. A janela respetiva é aberta e poderá configurar o serviço selecionado, ou seja, o LinkScanner Surf-Shield ou a Proteção Online. Na interface de definições avançadas pode editar toda a configuração de cada serviço de segurança do **AVG Internet Security**, mas qualquer configuração deve ser efetuada apenas por utilizadores experientes!

Seta – Utilize a seta verde na parte superior esquerda da janela para voltar à interface de utilizador principal com a síntese dos componentes.

6.3. Proteção de Identidade

O componente ***Proteção de Identidade*** executa o serviço ***Proteção de Identidade***, que protege continuamente os seus recursos digitais contra ameaças novas e desconhecidas existentes na Internet:

- A ***Proteção de Identidade*** é um serviço anti-malware que o protege de todos os tipos de malware (*spyware, bots, roubo de identidade, etc.*) utilizando tecnologias comportamentais e proporciona proteção imediata contra novos vírus. A Proteção de Identidade destina-se a evitar que ladrões de identidade roubem as suas palavras-passe, detalhes de contas bancárias, números de cartões de crédito e outros valores digitais pessoais por meio de todos os tipos de software malicioso *(malware)* que atacam o seu PC. Assegura o funcionamento correto de todos os programas em execução no seu computador ou na sua rede partilhada. A Proteção de Identidade identifica e bloqueia continuamente comportamentos suspeitos e protege o seu computador contra todo o novo malware. A Proteção de Identidade proporciona proteção em tempo real do seu computador contra ameaças novas e, inclusivamente, ameaças desconhecidas. Monitoriza todos os processos *(incluindo os ocultos)* e mais de 285 padrões de comportamento diferentes, podendo ainda determinar se algo malicioso está a acontecer no seu sistema. Desta forma, pode revelar ameaças ainda não descritas na base de dados de vírus. Sempre que um pedaço de código desconhecido chega ao computador, é imediatamente analisado em função de comportamento malicioso e rastreado. Se o ficheiro for considerado malicioso, a Proteção de Identidade remove o código para a Quarentena de Vírus e anula quaisquer alterações que tenham sido feitas ao sistema *(injeções de código, alterações ao registo, abertura de portas, etc.)*. Não é preciso iniciar uma análise para se manter protegido. A tecnologia é muito pró-ativa, raramente precisa de ser atualizada e está sempre de vigia.

Controlos da janela

Pode encontrar os seguintes controlos na janela:

Ativado / Desativado – O botão poderá fazer lembrar as luzes de um semáforo, tanto no aspeto como na funcionalidade. Clique uma vez para alternar entre as duas posições. A cor verde indica o estado ***Ativado***, que significa que o serviço de segurança Proteção de Identidade está ativo e totalmente funcional. A cor vermelha representa o estado ***Desativado***, ou seja, o serviço está desativado. Se não tiver um motivo aceitável para desativar o serviço, recomendamos que mantenha as predefinições de toda a configuração de segurança. As predefinições asseguram o desempenho ideal da aplicação e a segurança máxima do utilizador. Se por algum motivo pretender desativar o serviço, será avisado imediatamente da possibilidade de risco através da indicação ***Aviso*** a vermelho e da informação de que não se encontra totalmente protegido de momento. ***Tenha em atenção que deverá reativar o serviço o mais rapidamente possível!***

Definições – Clique no botão para ser redirecionado para a interface de definições avançadas. A janela respetiva é aberta e poderá configurar o serviço selecionado, ou seja, a Proteção de Identidade. Na interface de definições avançadas pode editar toda a configuração de cada serviço de segurança do **AVG Internet Security**, mas qualquer configuração deve ser efetuada apenas por utilizadores experientes!

Seta – Utilize a seta verde na parte superior esquerda da janela para voltar à interface de utilizador principal com a síntese dos componentes.

Infelizmente, o serviço Identity Alert não está incluído no **AVG Internet Security**. Se quiser utilizar esse tipo de proteção, utilize o botão ***Atualizar para ativar*** para ser redirecionado para a página Web dedicada, na qual poderá adquirir a licença do serviço Identity Alert.

Tenha em atenção que, mesmo com edições AVG Premium Security, o serviço Identity Alert só está disponível atualmente em algumas regiões: EUA, Reino Unido, Canadá e Irlanda..

6.4. Proteção de E-mail

O componente ***Proteção de E-mail*** abrange os dois serviços de segurança seguintes: ***Verificador de E-mail*** e ***Anti-Spam*** *(o serviço Anti-Spam só está disponível nas edições Internet/Premium Security)*.

- ***Verificador de E-mail***: uma das origens mais comuns de vírus e cavalos de Troia é o e-mail. O phishing e o spam fazem dos e-mails uma fonte ainda maior de riscos. As contas de e-mail gratuitas têm maiores probabilidades de receber e-mails maliciosos *(uma vez que raramente utilizam tecnologia anti-spam)* e os utilizadores domésticos dependem em grande parte de tais contas. Além disso, os utilizadores domésticos, ao navegarem por websites desconhecidos e ao preencherem formulários online com dados pessoais *(como o seu endereço de e-mail)*, aumentam a exposição a ataques através de e-mail. As empresas utilizam contas de e-mail empresariais e utilizam filtros anti-spam, etc., para reduzir o risco. O componente Proteção de E-mail é responsável pela análise de todas as mensagens de e-mail enviadas ou recebidas; sempre que for detetado um vírus num e-mail, é removido imediatamente para a Quarentena de Vírus. O componente também pode filtrar determinados tipos de anexos de e-mail e adicionar um texto de certificação às mensagens que não contenham infeções. ***O Verificador de E-mail não se destina a plataformas de servidores!***

- ***O componente Anti-Spam*** analisa todas as mensagens de e-mail a receber e assinala e-mails não solicitados como spam *(O termo Spam refere-se a e-mail não solicitado, normalmente utilizado para publicitar um produto ou serviço, que é enviado em massa para um grande número de endereços de e-mail ao mesmo tempo, enchendo as caixas de correio dos destinatários. Spam não se refere a correio eletrónico comercial legítimo, consentido pelos consumidores.)*. O Anti-Spam pode modificar o assunto do e-mail *(que foi identificado como sendo spam)* ao adicionar uma linha de texto especial. Poderá depois filtrar facilmente os e-mails no seu cliente de e-mail. O componente Anti-Spam utiliza vários métodos de análise para processar cada e-mail, proporcionando o máximo de proteção possível contra e-mails indesejados. O Anti-Spam utiliza uma base de dados que é atualizada regularmente para a deteção de spam. Também é possível utilizar os Servidores RBL *(bases de dados públicas de endereços de e-mail de "spammers conhecidos")* e adicionar manualmente endereços de e-mail à Lista Branca *(nunca marcar como spam)* e à Lista Negra *(marcar sempre como spam)*.

Controlos da janela

Para alternar entre as duas secções da janela, pode simplesmente clicar em qualquer parte do painel do serviço respetivo. O painel fica realçado com um tom de azul mais claro. Pode encontrar os controlos que se seguem nas duas secções da janela. A funcionalidade dos controlos é igual independentemente do serviço de segurança a que pertençam *(Verificador de E-mail ou Anti-Spam)*:

Ativado / Desativado – O botão poderá fazer lembrar as luzes de um semáforo, tanto no aspeto como na funcionalidade. Clique uma vez para alternar entre as duas posições. A cor verde indica o estado ***Ativado***, que significa que o serviço de segurança está ativo e totalmente funcional. A cor vermelha representa o estado ***Desativado***, ou seja, o serviço está desativado. Se não tiver um motivo aceitável para desativar o serviço, recomendamos que mantenha as predefinições de toda a configuração de segurança. As predefinições asseguram o desempenho ideal da aplicação e a segurança máxima do utilizador. Se por algum motivo pretender desativar o serviço, será avisado imediatamente da possibilidade de risco através da indicação ***Aviso*** a vermelho e da informação de que não se encontra totalmente protegido de momento. ***Tenha em atenção que deverá reativar o serviço o mais rapidamente possível!***

Definições – Clique no botão para ser redirecionado para a interface de definições avançadas. A janela respetiva é aberta e poderá configurar o serviço selecionado, ou seja, o Verificador de E-mail ou o Anti-Spam. Na interface de definições avançadas pode editar toda a configuração de cada serviço de segurança do **AVG Internet Security**, mas qualquer configuração deve ser efetuada apenas por utilizadores experientes!

Seta – Utilize a seta verde na parte superior esquerda da janela para voltar à interface de utilizador principal com a síntese dos componentes.

6.5. Firewall

Uma ***Firewall*** é um sistema que implementa uma política de controlo de acesso entre duas ou mais redes, bloqueando/autorizando o tráfego. A Firewall contém um conjunto de regras que protege a rede interna de ataques provenientes do *exterior (normalmente da Internet)* e controla todas as comunicações em cada porta da rede. A comunicação é avaliada de acordo com as regras definidas, sendo então permitida ou proibida. Se a Firewall detetar alguma tentativa de intrusão, "bloqueia" a tentativa e não deixa o intruso aceder ao computador. A Firewall está configurada para permitir ou negar comunicações internas/externas *(ambos os sentidos, entrada e saída)* através das portas definidas e para as aplicações de software definidas. Por exemplo, a firewall pode ser configurada para permitir apenas o fluxo de entrada ou saída de dados da Internet utilizando o Microsoft Explorer. Qualquer tentativa de transmissão de dados da Internet por qualquer outro browser será bloqueada. A Firewall protege a sua informação de identificação pessoal de ser enviada do seu computador sem a sua autorização. Controla a forma como é efetuada a comunicação de dados entre o seu computador e outros computadores da Internet ou da rede local. Dentro de uma organização, a Firewall também protege computadores individuais de ataques desencadeados por utilizadores internos ou por outros computadores da rede.

No **AVG Internet Security**, a ***Firewall*** controla todo o tráfego em todas as portas de rede do seu computador. Com base nas regras definidas, a Firewall avalia as aplicações que estão a funcionar no seu computador *(e que pretendem estabelecer ligação à rede local ou à Internet)* ou as aplicações que tentam estabelecer ligação ao seu PC a partir do exterior. Para cada uma dessas aplicações, a Firewall permite ou proíbe as comunicações através das portas da rede. Por predefinição, se a aplicação for desconhecida *(ou seja, se não tiver regras da Firewall definidas)*, a Firewall perguntar-lhe-á se pretende permitir ou bloquear a

tentativa de comunicação.

A Firewall do AVG não se destina a proteção de plataformas de servidores!

Recomendação: *regra geral, não é recomendável utilizar mais de uma firewall num mesmo computador. A segurança do computador não é potenciada se instalar mais firewalls. É, na verdade, mais provável que ocorram alguns conflitos entre estas duas aplicações. Como tal, é recomendável que utilize apenas uma firewall no seu computador e desative todas as outras, eliminando desta forma o risco de possíveis conflitos e quaisquer problemas associados.*

Nota: *após a instalação do AVG Internet Security, poderá ser necessário reiniciar o computador para ativar o componente Firewall. Nesse caso, aparece a janela do componente a informar que é necessário reiniciar o computador. Nessa janela poderá encontrar o botão* ***Reiniciar agora****. Até o computador ser reiniciado, o componente Firewall não estará totalmente ativado. Além disso, todas as opções de edição na janela também estarão desativadas. Preste atenção ao aviso e reinicie o computador o mais rapidamente possível!*

Modos da Firewall disponíveis

A Firewall permite-lhe definir regras de segurança específicas consoante o seu computador esteja localizado num domínio, seja um computador independente ou mesmo um portátil. Cada uma destas opções requer um nível de proteção diferente, sendo os níveis abrangidos pelos respetivos modos. Resumindo, um modo da Firewall é uma configuração específica do componente Firewall, e pode usar uma variedade dessas configurações predefinidas.

- ***Automático*** – neste modo, a Firewall lida com todo o tráfego de rede automaticamente. O utilizador não terá de tomar qualquer decisão. A Firewall permitirá a ligação para cada aplicação conhecida e, ao mesmo tempo, será criada uma regra para a aplicação que especifica que a aplicação pode sempre estabelecer ligação no futuro. No caso de outras aplicações, a Firewall decide se a ligação deve ser permitida ou bloqueada com base no comportamento da aplicação. No entanto, numa situação desse tipo, a regra não será criada e a aplicação será verificada novamente quando tentar estabelecer ligação. O modo automático é extremamente discreto e é o modo recomendado para a maioria dos utilizadores.

- ***Interativo*** – este modo é útil se pretender ter controlo total sobre todo o tráfego de rede que entra e sai do computador. A Firewall monitorizará o tráfego e avisá-lo-á se houver qualquer tentativa de comunicação ou transferência de dados, podendo depois permitir ou bloquear a tentativa conforme necessário. Recomendado apenas a utilizadores avançados.

- ***Bloquear o acesso à Internet*** – a ligação à Internet é totalmente bloqueada; deixa de poder aceder à Internet e ninguém do exterior pode aceder ao computador. Apenas para uso especial e de tempo limitado.

- ***Desligar a proteção da firewall (não recomendado)*** – desativar a Firewall possibilitará o fluxo de todo o tráfego de rede do e para o computador. Consequentemente, o computador ficará mais vulnerável a ataques de piratas informáticos. Pense bem antes de selecionar esta opção.

Tenha em consideração um modo automático específico que também está disponível na Firewall. Esse modo é ativado silenciosamente se o componente Computador ou Proteção de Identidade for desativado e se o computador ficar mais vulnerável como consequência desse facto. Nesses casos, a Firewall permitirá automaticamente apenas aplicações conhecidas e totalmente seguras. Ser-lhe-á pedida uma decisão no que diz respeito a todas as outras aplicações. Esta medida destina-se a compensar a proteção desativada e a manter o seu computador protegido.

Recomendamos que não desative a Firewall de todo! Contudo, se for realmente necessário desativar o componente Firewall, poderá fazê-lo selecionando o modo "Desligar a proteção da firewall" na lista acima de modos de Firewall disponíveis.

Controlos da janela

A janela apresenta uma síntese de informações básicas relativas ao estado do componente Firewall:

- ***Modo da firewall*** – Apresenta informação relativa ao modo da Firewall que está selecionado. Utilize o botão ***Alterar*** que se encontra ao lado da informação apresentada para mudar para a interface de Definições da Firewall se pretender alterar o modo atual *(para ver uma descrição e recomendações de utilização dos perfis da Firewall, consulte o parágrafo anterior)*.

- ***Partilha de ficheiros e impressoras*** – Indica se a partilha de ficheiros e impressoras *(em ambos os sentidos)* é permitida de momento. Partilha de ficheiros e de impressoras significa, efetivamente, partilhar ficheiros ou pastas que sejam assinalados como "Partilhados" no Windows, em unidades de disco comuns, impressoras, digitalizadores e dispositivos semelhantes. A partilha desses itens só deverá ser feita dentro de redes que possam ser consideradas seguras *(por exemplo, em casa, no trabalho ou na escola)*. No entanto, se estiver ligado a uma rede pública *(como a rede Wi-Fi de um aeroporto ou um café com Internet)*, poderá não ser aconselhável partilhar seja o que for.

- ***Ligado a*** – Apresenta informação relativa ao nome da rede à qual o computador está ligado. No sistema operativo Windows XP, o nome da rede corresponde à designação selecionada para a rede específica aquando da primeira ligação do computador à rede. No sistema operativo Windows Vista ou superior, o nome da rede é retirado automaticamente do Centro de Rede e Partilha.

- ***Repor predefinição*** – Clique neste botão para substituir a configuração atual da Firewall e repor a configuração predefinida baseada em deteção automática.

A janela contém os seguintes controlos gráficos:

Definições – Clique no botão para ser redirecionado para a interface de Definições da Firewall,

onde pode editar toda a configuração da Firewall. Qualquer configuração deverá ser efetuada exclusivamente por utilizadores avançados!

Seta – Utilize a seta verde na parte superior esquerda da janela para voltar à interface de utilizador principal com a síntese dos componentes.

6.6. Analisador do PC

O componente ***Analisador do PC*** é uma ferramenta avançada que permite analisar e corrigir o sistema detalhadamente de modo a melhorar a velocidade e o desempenho geral do computador. É iniciado através do botão ***Corrigir desempenho*** que se encontra na janela da interface de utilizador principal ou através da opção com o mesmo nome que aparece no menu de contexto do ícone do AVG na barra de tarefas. Poderá, então, visualizar o progresso da análise e os resultados da mesma diretamente na tabela:

É possível analisar as seguintes categorias: erros do registo, ficheiros redundantes, fragmentação e atalhos inválidos:

- ***Erros do Registo*** apresenta o número de erros no Registo do Windows que podem estar a tornar o computador lento ou a causar o aparecimento de mensagens de erro.
- ***Ficheiros Redundantes*** apresenta o número de ficheiros que ocupam espaço no disco e que provavelmente podem ser eliminados. Normalmente, esses ficheiros são vários tipos de ficheiros temporários e ficheiros da Reciclagem.
- ***Fragmentação*** calcula a percentagem do disco rígido que está fragmentada, ou seja, usada prolongadamente, de tal forma que a maioria dos ficheiros está espalhada por várias secções do disco físico.
- ***Atalhos Inválidos*** deteta atalhos que já não funcionam, que conduzem a localizações não existentes, etc.

A síntese dos resultados apresenta o número de problemas detetados no sistema, classificados consoante as categorias de teste respetivas. Os resultados da análise também serão apresentados graficamente num eixo,

na coluna ***Gravidade***.

Botões de controlo

- ***Parar análise*** (*apresentado durante a execução da análise*) – clique neste botão para interromper a análise do computador.

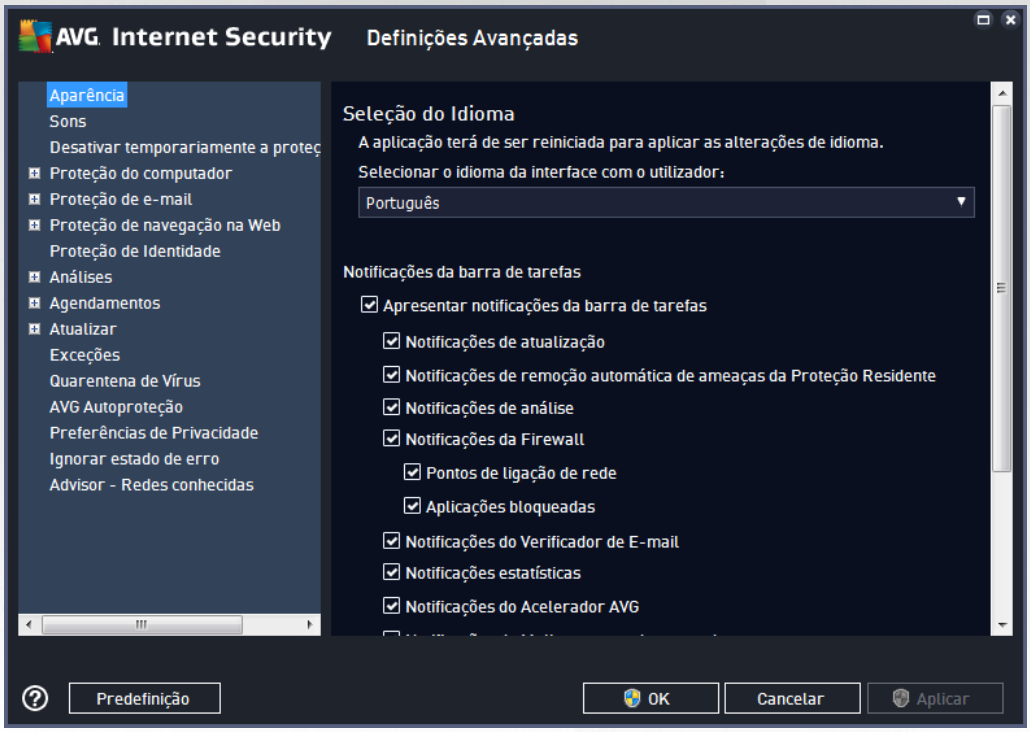
- ***Corrigir agora*** *(apresentado após a conclusão da análise*) – Infelizmente, a funcionalidade do Analisador do PC no **AVG Internet Security** está limitada à análise do estado atual do PC. Contudo, a AVG disponibiliza uma ferramenta avançada que permite analisar e corrigir o sistema detalhadamente de modo a melhorar a velocidade e o desempenho geral do computador. Clique no botão para aceder ao site dedicado e obter mais informações.

7. Definições Avançadas do AVG

A janela de configuração avançada do **AVG Internet Security** abre numa nova janela com a identificação ***Definições Avançadas do AVG***. A janela está dividida em duas secções: a parte esquerda disponibiliza uma navegação esquematizada em árvore às opções de configuração do programa. Selecione o componente cuja configuração pretende alterar (*ou a parte específica do componente*) para abrir a janela de edição na secção do lado direito.

7.1. Aparência

O primeiro item da árvore de navegação, ***Aparência***, refere-se às definições gerais da interface de utilizador do **AVG Internet Security** e disponibiliza algumas opções básicas do comportamento da aplicação:



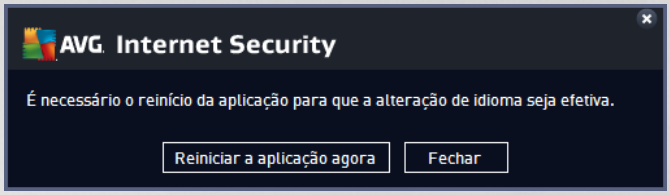
Seleção do Idioma

Na secção ***Seleção do Idioma*** pode escolher o idioma pretendido a partir do menu de opções. O idioma selecionado será então usado para toda a interface de utilizador do **AVG Internet Security**. O menu de opções só apresenta os idiomas que o utilizador tiver selecionado previamente para instalação durante o processo de instalação e o idioma Inglês (*que é sempre instalado automaticamente por predefinição*). Para concluir a alteração do idioma do **AVG Internet Security**, é necessário reiniciar a aplicação. Proceda do seguinte modo:

- No menu de opções, selecione o idioma pretendido para a aplicação
- Confirme a seleção clicando no botão ***Aplicar*** *(canto inferior direito da janela)*
- Clique no botão ***OK*** para confirmar

- É apresentada uma nova janela a informá-lo de que para alterar o idioma da aplicação, é necessário reiniciar o seu **AVG Internet Security**

- Clique no botão ***Reiniciar o AVG agora*** para aceitar o reinício do programa e aguarde alguns instantes para que a alteração do idioma seja aplicada:


AVG Internet Security
É necessário o reinício da aplicação para que a alteração de idioma seja efetiva.
Reiniciar a aplicação agora
Fechar

Notificações da barra de tarefas

Nesta secção pode suprimir a apresentação de notificações da barra de tarefas relativas ao estado da aplicação **AVG Internet Security**. Por predefinição, as notificações do sistema estão definidas como permitidas. Recomendamos vivamente que mantenha esta configuração! As notificações do sistema disponibilizam informações relativas, por exemplo, à execução do processo de análise ou atualização, ou a alterações do estado de um componente do **AVG Internet Security**. Estas notificações são sempre importantes!

No entanto, se por algum motivo decidir que não quer que estas informações sejam apresentadas ou que só quer ver determinadas notificações *(relacionadas com um componente específico do AVG Internet Security)*, pode definir e especificar as suas preferências marcando/desmarcando as seguintes opções:

- ***Apresentar notificações da barra de tarefas*** *(ativado por predefinição)* – por predefinição, todas as notificações são apresentadas. Desmarque este item para desativar por completo a apresentação das notificações do sistema. Quando ativado, pode ainda especificar quais as notificações específicas que devem ser apresentadas.

    - ***Notificações de atualização*** *(ativado por predefinição)* – decida se devem ser apresentadas informações relativas à execução, ao progresso e à finalização do processo de atualização do **AVG Internet Security**.

    - ***Notificações de remoção automática de ameaças da Proteção Residente*** *(ativado por predefinição)* – decida se devem ser apresentadas ou ocultadas informações relativas aos processos de guardar, copiar e abrir ficheiros (*esta configuração só aparece se a opção de restauro automático da Proteção Residente estiver ativada*).

    - ***Notificações de análise*** *(ativado por predefinição)* – decida se devem ser apresentadas informações relativas ao início automático da análise agendada, o seu progresso e resultados.

    - ***Notificações da Firewall*** *(ativado por predefinição)* – decida se devem ser apresentadas informações relativas ao estado e aos processos da Firewall (ex.: avisos de ativação/ desativação do componente, possível bloqueio de tráfego, etc.). Este item disponibiliza mais duas opções de seleção específicas *(para uma explicação detalhada de cada uma delas, consulte o capítulo Firewall deste documento)*:

        – ***Pontos de ligação de rede*** *(desativado por predefinição)* – quando é estabelecida a ligação a uma rede, a Firewall informa se conhece a rede e de que forma será definida a partilha de ficheiros e impressoras.

– ***Aplicações bloqueadas*** *(ativado por predefinição)* – quando uma aplicação desconhecida ou suspeita tenta estabelecer ligação a uma rede, a Firewall bloqueia a tentativa e apresenta uma notificação. Esta medida é útil para o manter informado, por isso recomendamos que mantenha sempre esta funcionalidade ativada.

- ***Notificações do Verificador de E-mail*** *(ativado por predefinição)* – decida se devem ser apresentadas informações relativas à execução da análise de todas as mensagens de e-mail de entrada e saída.

- ***Notificações estatísticas*** *(ativado por predefinição)* – mantenha a opção marcada para permitir a apresentação de notificações estatísticas na barra de tarefas.

- ***Notificações do Acelerador AVG*** *(ativado por predefinição)* – decida se devem ser apresentadas informações relativas às atividades do ***Acelerador AVG***. O serviço ***Acelerador AVG*** permite uma reprodução de vídeos online mais fluida e facilita as transferências.

- ***Notificações do melhoramento do tempo de arranque*** *(desativado por predefinição)* – decida se pretende ser informado relativamente à aceleração do tempo de arranque do computador.

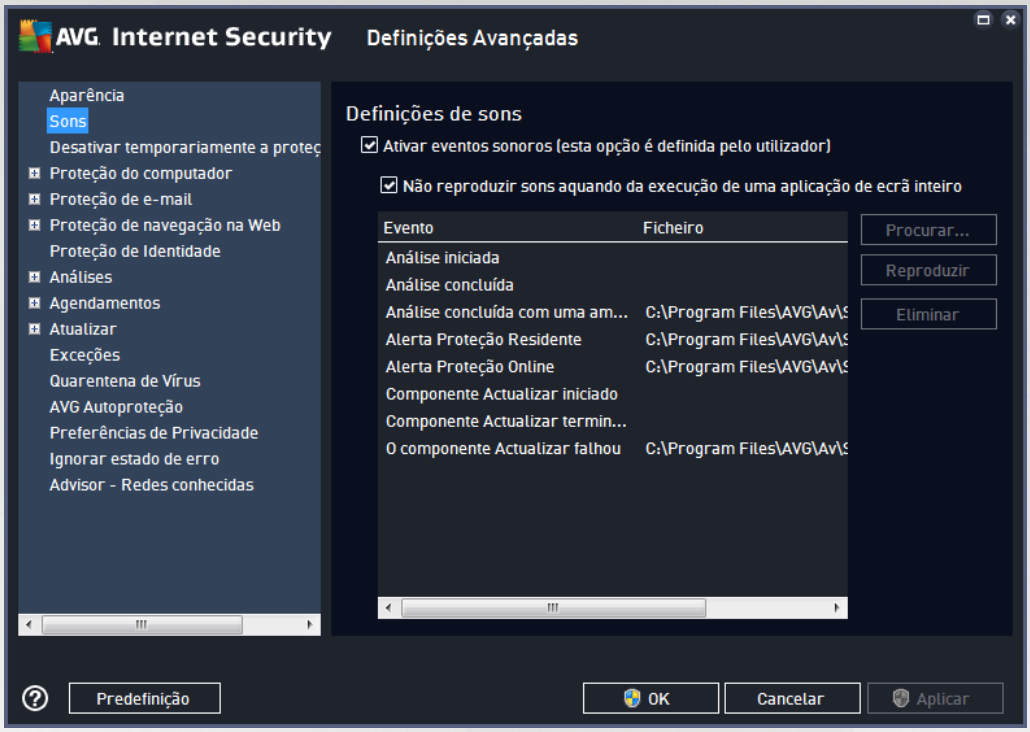
- ***Notificações do Conselho do AVG*** *(ativado por predefinição)* – decida se as informações relativas às atividades do Conselho do AVG devem ser apresentadas no painel deslizante que aparece na barra de tarefas.

Modo de jogo

Esta função destina-se a aplicações de ecrã inteiro em que a apresentação de quaisquer janelas de informação do AVG (*apresentadas, por exemplo, quando uma análise agendada é iniciada*) seria incómoda (*poderiam minimizar a aplicação ou corromper os seus gráficos*). Para evitar esta situação, mantenha a caixa de verificação da opção ***Ativar o Modo de jogo aquando da execução de uma aplicação de ecrã inteiro*** marcada (*predefinição*).

7.2. Sons

Na janela ***Definições de sons*** pode especificar se quer ser informado de ações específicas do **AVG Internet Security** por meio de uma notificação sonora:



As definições só são válidas para a conta de utilizador atual; ou seja, cada utilizador do computador pode ter as suas próprias definições de sons. Se quiser permitir a notificação sonora, mantenha a opção ***Ativar eventos sonoros*** marcada (*a opção está ativada por predefinição*) para ativar a lista de todas as ações relevantes. Também pode querer marcar a opção ***Não reproduzir sons aquando da execução de uma aplicação de ecrã inteiro*** para suprimir a notificação sonora em situações em que o evento possa ser perturbador *(consulte também a secção Modo de jogo no capítulo Definições avançadas/Aparência deste documento)*.

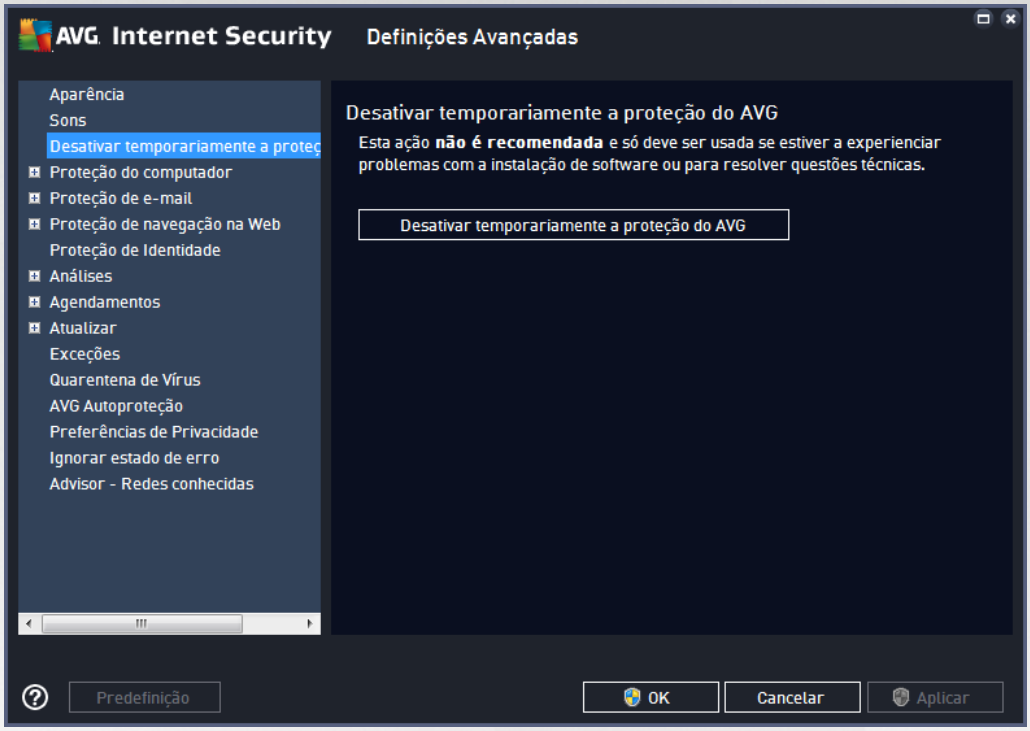
Botões de controlo

- ***Procurar...*** – depois de selecionar o respetivo evento na lista, utilize o botão ***Procurar*** para procurar no disco o ficheiro de som que pretende atribuir ao evento. *(Tenha em atenção que só são suportados sons no formato *.wav!)*
- ***Reproduzir*** – para ouvir o som selecionado, realce o evento na lista e clique no botão ***Reproduzir***.
- ***Eliminar*** – utilize o botão ***Eliminar*** para remover o som atribuído a um evento específico.

7.3. Desativar temporariamente a proteção do AVG

Na janela ***Desativar temporariamente a proteção do AVG*** existe a possibilidade de desativar toda a proteção oferecida pelo **AVG Internet Security** de uma só vez.

Tenha em atenção que não deverá usar esta opção a menos que seja absolutamente necessário!

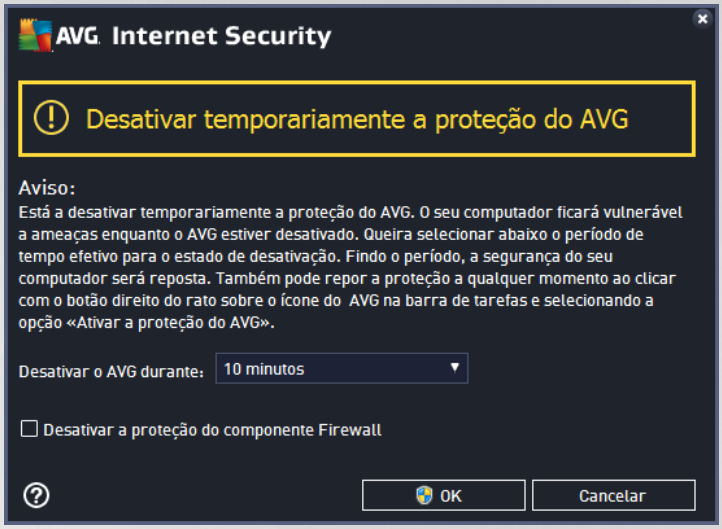


Na maioria dos casos, ***não é necessário*** desativar o **AVG Internet Security** antes de instalar novo software ou controladores, mesmo que o instalador ou o assistente do software sugiram que os programas e aplicações em execução devam ser encerrados primeiro para garantir que não ocorrem interrupções durante o processo de instalação. Caso se depare com problemas durante a instalação, experimente primeiro desativar a proteção residente *(desmarque o item **Ativar a Proteção Residente** na janela mostrada quando clica na ligação)*. Se tiver de desativar o **AVG Internet Security** temporariamente, deverá voltar a ativá-lo assim que terminar. Se estiver ligado à Internet ou a uma rede quando o software antivírus estiver desativado, o seu computador estará vulnerável a ataques.

Como desativar a proteção do AVG

Assinale a caixa ***Desativar temporariamente a proteção do AVG*** e confirme a sua opção clicando no botão ***Aplicar***. Na janela ***Desativar temporariamente a proteção do AVG*** especifique a duração da desativação do **AVG Internet Security**. Por predefinição, a proteção será desativada durante 10 minutos, o que deve ser suficiente para qualquer tarefa comum como a instalação de novo software, etc. Pode optar por um período de tempo mais longo; no entanto, essa opção não é recomendada se não for absolutamente necessária. Posteriormente, todos os componentes desativados serão ativados de novo automaticamente. No máximo, pode desativar a proteção do AVG até ao próximo reinício do computador. Existe uma opção separada de desativação do componente ***Firewall*** incluída na janela ***Desativar temporariamente a proteção do AVG***.

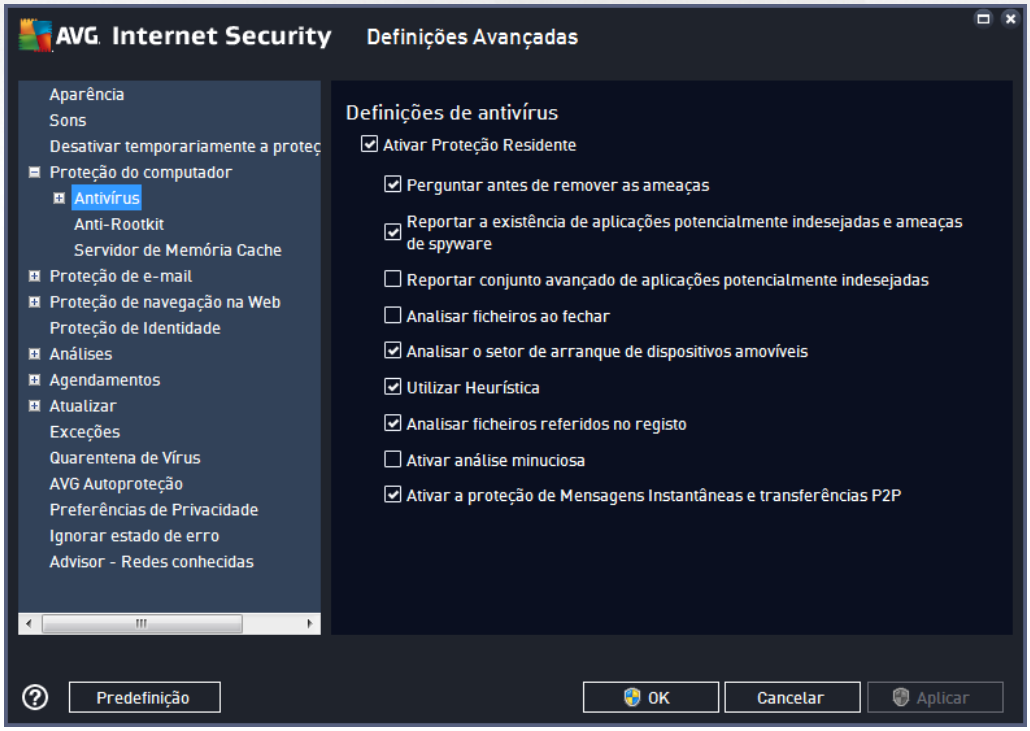
Assinale a caixa ***Desativar a proteção do componente Firewall*** para tal.


AVG Internet Security
Desativar temporariamente a proteção do AVG
Aviso:
Está a desativar temporariamente a proteção do AVG. O seu computador ficará vulnerável a ameaças enquanto o AVG estiver desativado. Queira selecionar abaixo o período de tempo efetivo para o estado de desativação. Findo o período, a segurança do seu computador será reposta. Também pode repor a proteção a qualquer momento ao clicar com o botão direito do rato sobre o ícone do AVG na barra de tarefas e selecionando a opção «Ativar a proteção do AVG».
Desativar o AVG durante:
10 minutos
Desativar a proteção do componente Firewall
OK
Cancelar

7.4. Proteção do computador

7.4.1. Antivírus

O componente ***Antivírus***, juntamente com a ***Proteção Residente***, protege o seu computador continuamente contra todos os tipos conhecidos de vírus, spyware e malware em geral *(incluindo o chamado malware latente e inativo, ou seja, malware que foi transferido, mas que ainda não foi ativado)*.



Na janela ***Definições da Proteção Residente*** pode ativar ou desativar a Proteção Residente completamente ao marcar/desmarcar o item ***Ativar a Proteção Residente*** (*esta opção está ativada por predefinição*). Além disso, pode selecionar as funcionalidades da proteção residente que deverão ser ativadas:

- ***Perguntar antes de remover as ameaças*** (*ativado por predefinição*) – marque esta opção para garantir que a Proteção Residente não realiza qualquer ação automaticamente; em vez disso, apresenta uma janela com a descrição da ameaça detetada, permitindo-lhe decidir o que pretende fazer. Se deixar a caixa desmarcada, o **AVG Internet Security** removerá automaticamente a infeção; se tal não for possível, o objeto será movido para a Quarentena de Vírus.

- ***Reportar aplicações potencialmente indesejadas e ameaças de spyware*** (*ativado por predefinição*) – marque esta opção para ativar a análise que procura spyware e também vírus. O Spyware representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade ativada, uma vez que aumenta a segurança do seu computador.

- ***Reportar conjunto avançado de aplicações potencialmente indesejadas*** (*desativado por predefinição*) – marque esta opção para detetar pacotes expandidos de spyware: programas que são perfeitamente fidedignos e inofensivos quando adquiridos diretamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, pode potencialmente bloquear programas legais e está, como tal, desativada por predefinição.

- ***Analisar ficheiros ao fechar*** (*desativado por predefinição*) – a análise ao fechar assegura que o AVG analisa objetos ativos (ex.: aplicações, documentos...) quando estes são abertos e também quando são fechados; esta funcionalidade ajuda a proteger o seu computador contra alguns tipos de vírus sofisticados.

- ***Analisar o setor de arranque de dispositivos amovíveis*** (*ativado por predefinição*) – marque esta opção para verificar a existência de ameaças nos setores de arranque de unidades flash USB, unidades de disco externo e outros suportes amovíveis ligados ao computador.

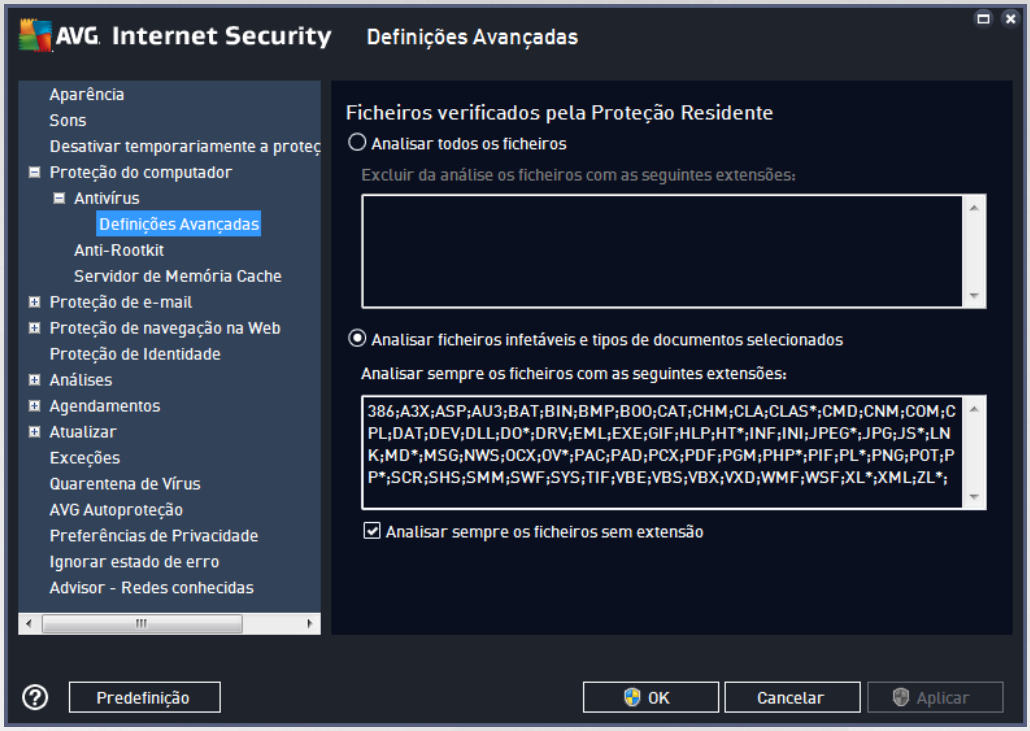
- ***Utilizar Heurística*** (*ativado por predefinição*) – a análise heurística será utilizada para deteção (*emulação dinâmica das instruções do objeto analisado num ambiente de computador virtual*).

- ***Analisar ficheiros referidos no registo*** (*ativado por predefinição*) – este parâmetro define que o AVG irá analisar todos os ficheiros executáveis adicionados ao registo de arranque para evitar a execução de infeções conhecidas aquando do próximo arranque do computador.

- ***Ativar análise minuciosa*** (*desativado por predefinição*) – em situações específicas (*num estado extremo de emergência*) pode marcar esta opção para ativar os mais rigorosos algoritmos que irão verificar aprofundadamente a existência de objetos perigosos. Tenha em consideração que este método é bastante demorado.

- ***Ativar a proteção de Mensagens Instantâneas e transferências P2P*** (*ativado por predefinição*) – marque este item se pretender confirmar que a comunicação através de mensagens instantâneas (*por exemplo, AIM, Yahoo!, ICQ, Skype, MSN Messenger...*) e os dados transferidos por intermédio de redes Ponto-a-Ponto *(redes que possibilitam uma ligação direta entre computadores-cliente, sem um servidor, o que poderá ser perigoso; é o método normalmente utilizado para partilhar ficheiros de música)* não têm vírus.

Na janela ***Ficheiros verificados pela Proteção Residente*** é possível configurar os ficheiros a analisar (*por extensões específicas*):

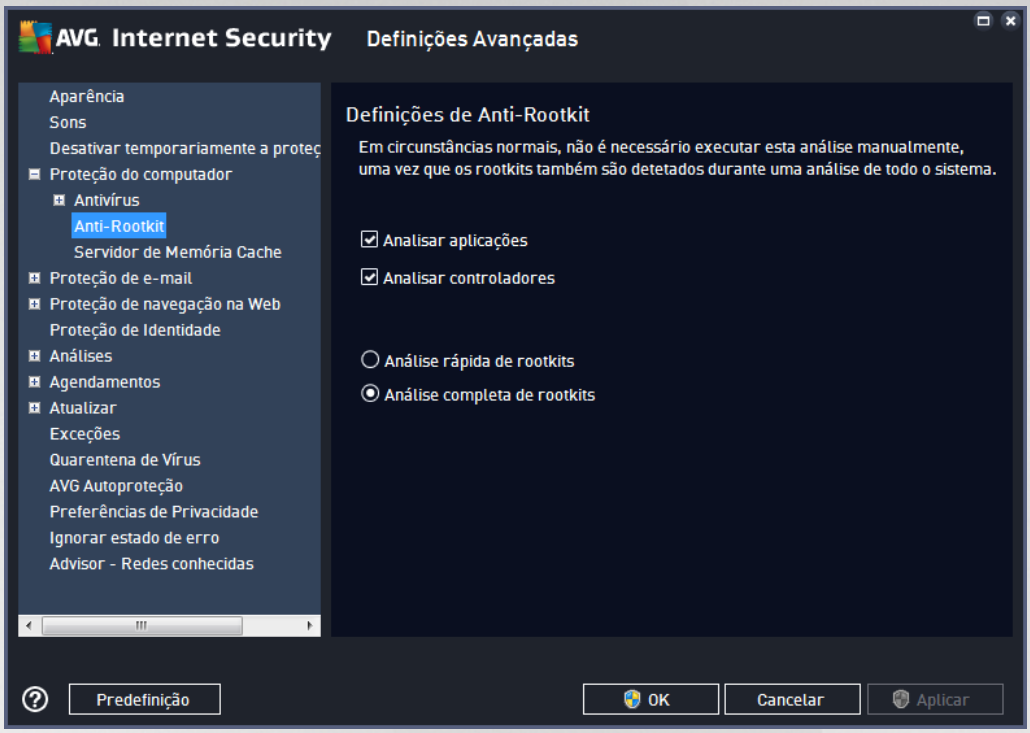


Marque a caixa respetiva para decidir se pretende ***Analisar todos os ficheiros*** ou apenas ***Analisar ficheiros infetáveis e tipos de documentos selecionados***. Para acelerar a análise e proporcionar ao mesmo tempo o nível máximo de proteção, recomendamos que mantenha as predefinições. Dessa forma, serão analisados apenas ficheiros infetáveis. Na secção respetiva da janela pode também encontrar uma lista editável de extensões que definem os ficheiros incluídos na análise.

Marque a caixa ***Analisar sempre os ficheiros sem extensão*** (*ativado por predefinição*) para assegurar a análise de ficheiros sem extensão e formato desconhecido pela Proteção Residente. Recomendamos que mantenha esta funcionalidade ativada, uma vez que os ficheiros sem extensão são suspeitos.

7.4.2. Anti-Rootkit

Na janela ***Definições de Anti-Rootkit*** pode editar a configuração do serviço ***Anti-Rootkit*** e parâmetros específicos da análise anti-rootkit. A análise anti-rootkit é um processo predefinido incluído na operação Analisar todo o computador:

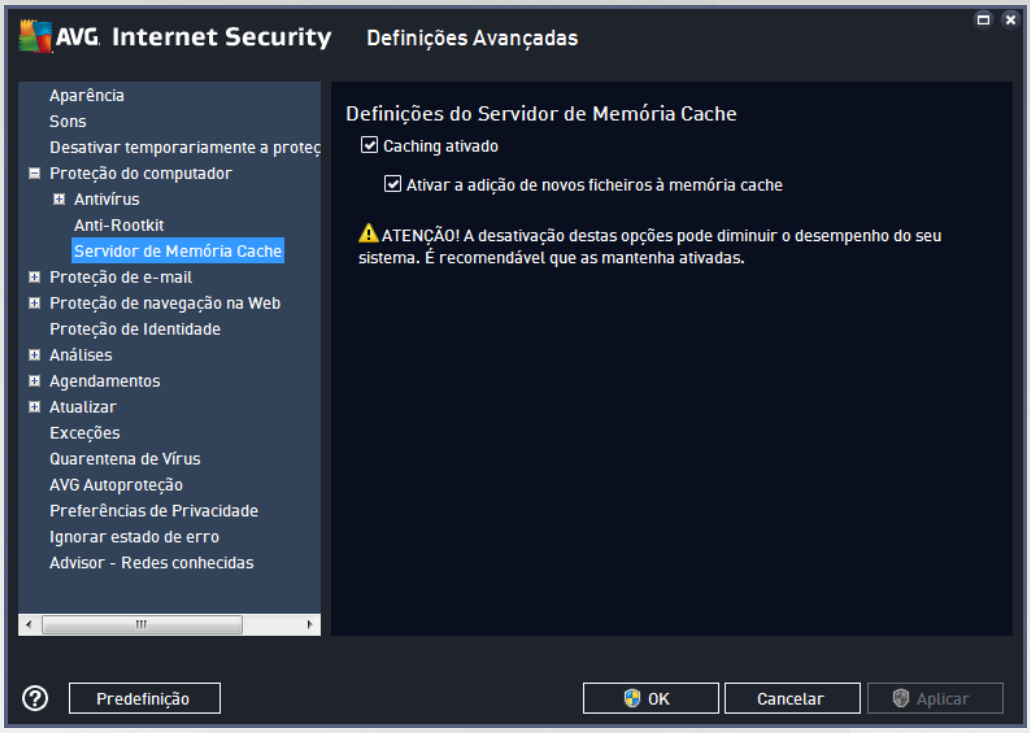


Analisar aplicações e ***Analisar controladores*** permitem-lhe especificar detalhadamente o que deve ser incluído na análise anti-rootkit. Estas definições são destinadas a utilizadores avançados; recomendamos que mantenha todas as opções ativadas. Também pode escolher o modo de análise de rootkits:

- ***Análise rápida de rootkits*** – analisa todos os processos em execução, controladores carregados e a pasta de sistema (*normalmente c:\Windows*)
- ***Análise completa de rootkits*** – analisa todos os processos em execução, controladores carregados, a pasta de sistema (*normalmente c:\Windows*) e todos os discos locais (*incluindo unidades flash, mas excluindo unidades de disquete/CD*)

7.4.3. Servidor de Memória Cache

A janela das ***Definições do Servidor de Memória Cache*** é referente ao processo do servidor de memória cache destinado a acelerar todos os tipos de análises do **AVG Internet Security**:



O servidor de memória cache recolhe e guarda as informações relativas a ficheiros fidedignos (*um ficheiro é considerado fidedigno se estiver assinado com uma assinatura digital emitida por uma fonte fidedigna*). Esses ficheiros são então automaticamente considerados seguros e não precisam de voltar a ser analisados; como tal, esses ficheiros são ignorados durante a análise.

A janela das ***Definições do Servidor de Memória Cache*** apresenta as seguintes opções de configuração:

- ***Caching ativado*** (*ativado por predefinição*) – desmarque a caixa para desativar o ***Servidor de Memória Cache*** e limpar a memória cache. Tenha em atenção que a análise pode ficar mais morosa, assim como o desempenho do computador, uma vez que todos os ficheiros em utilização serão analisados pela existência de vírus e spyware.

- ***Ativar a adição de novos ficheiros à memória cache*** (*ativado por predefinição*) – desmarque a caixa para parar a adição de mais ficheiros à memória cache. Quaisquer ficheiros já colocados na memória cache serão aí mantidos e utilizados até a ação de caching ser desativada por completo, ou até à próxima atualização da base de dados de vírus.

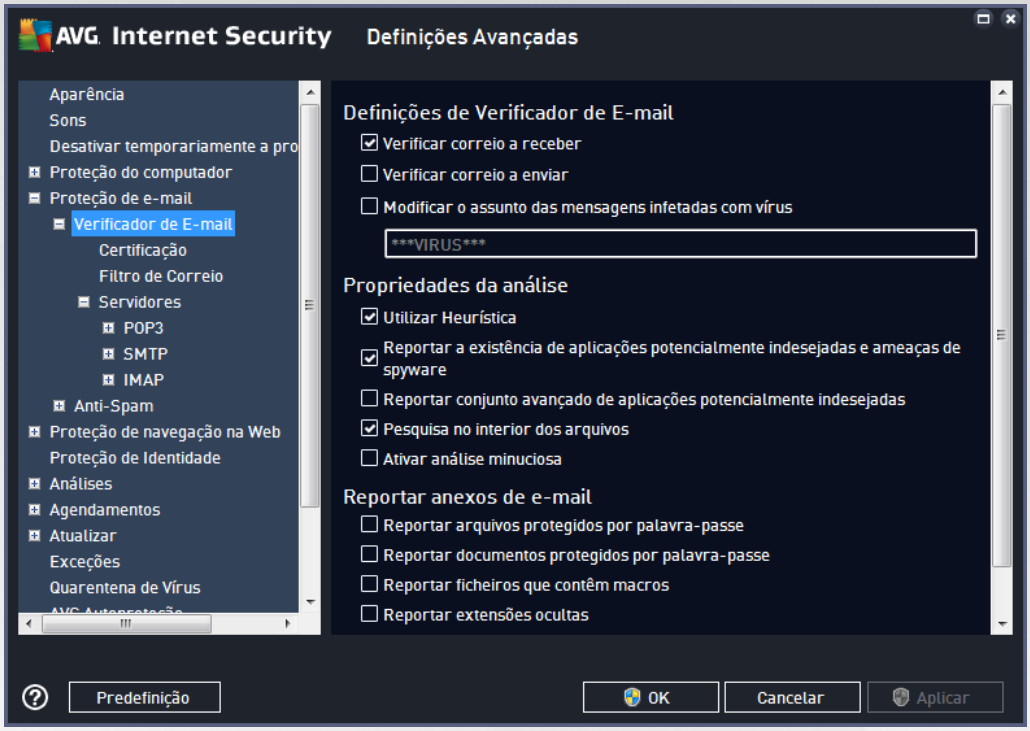
A menos que tenha uma boa razão para desativar o servidor de memória cache, recomendamos vivamente que mantenha as predefinições e deixe ambas as opções ativadas! Caso contrário, poderá ocorrer uma diminuição significativa da velocidade e desempenho do seu sistema.

7.5. Verificador de E-mail

Nesta secção pode editar a configuração detalhada do Verificador de E-mail e do Anti-Spam:

7.5.1. Verificador de E-mail

A janela ***Verificador de E-mail*** está dividida em três secções:



Análise de correio eletrónico

Nesta secção, pode configurar estas definições básicas para as mensagens de e-mail a receber e/ou a enviar:

- ***Verificar correio a receber*** (*ativado por predefinição*) – marque para ativar/desativar a opção de análise de todas as mensagens de e-mail entregues no seu cliente de e-mail
- ***Verificar correio a enviar*** (*desativado por predefinição*) – marque para ativar/desativar a opção de análise de todas as mensagens de e-mail enviadas a partir da sua conta
- ***Modificar o assunto das mensagens infetadas com vírus*** (*desativado por predefinição*) – se quiser ser informado quando uma mensagem for detetada como infetada, marque este item e preencha o texto pretendido no campo de texto. Este texto será então adicionado ao campo "Assunto" de cada e-mail detetado para uma identificação e filtragem mais fáceis. O valor predefinido é ***VIRUS***, que recomendamos que mantenha.

Propriedades da análise

Nesta secção, pode especificar como as mensagens de e-mail serão analisadas:

- ***Utilizar Heurística*** (*ativado por predefinição*) – marque esta opção para usar o método de deteção da

análise heurística durante a análise de mensagens de e-mail. Quando esta opção está ativada, pode filtrar anexos de e-mail não só pela extensão, mas também pelos conteúdos do anexo. O filtro pode ser definido na janela Filtro de Correio.

- ***Reportar aplicações potencialmente indesejadas e ameaças de spyware*** (*ativado por predefinição*) – marque esta opção para ativar a análise que procura spyware e também vírus. O Spyware representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade ativada, uma vez que aumenta a segurança do seu computador.

- ***Reportar conjunto avançado de aplicações potencialmente indesejadas*** (*desativado por predefinição*) – marque esta opção para detetar pacotes expandidos de spyware: programas que são perfeitamente fidedignos e inofensivos quando adquiridos diretamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, poderá bloquear programas legais e está, como tal, desativada por predefinição.

- ***Pesquisa no interior dos arquivos*** (*ativado por predefinição*) – marque esta opção para analisar os conteúdos de arquivos anexados a mensagens de e-mail.

- ***Ativar análise minuciosa*** (*desativado por predefinição*) – em situações específicas (*ex.: suspeita de infeção do computador por um vírus ou ataque*) pode marcar esta opção para ativar os algoritmos de análise mais rigorosos que irão analisar todas as áreas do seu computador, incluindo as que dificilmente são infetadas, por precaução. Tenha em consideração que este método é bastante demorado.

Reportar anexos de e-mail

Nesta secção, pode configurar relatórios adicionais acerca de ficheiros potencialmente perigosos ou suspeitos. Tenha em atenção que não será apresentada qualquer janela de aviso; só será adicionado um texto de certificação no final do e-mail e todos esses relatórios serão listados na janela Deteção de Proteção de E-mail:

- ***Reportar arquivos protegidos por palavra-passe*** – arquivos (*ZIP, RAR, etc.*) que estão protegidos por palavra-passe não podem ser analisados pelo antivírus; marque a caixa para os reportar como potencialmente perigosos.

- ***Reportar documentos protegidos por palavra-passe*** – documentos que estão protegidos por palavra-passe não podem ser analisados pelo antivírus; marque a caixa para os reportar como potencialmente perigosos.

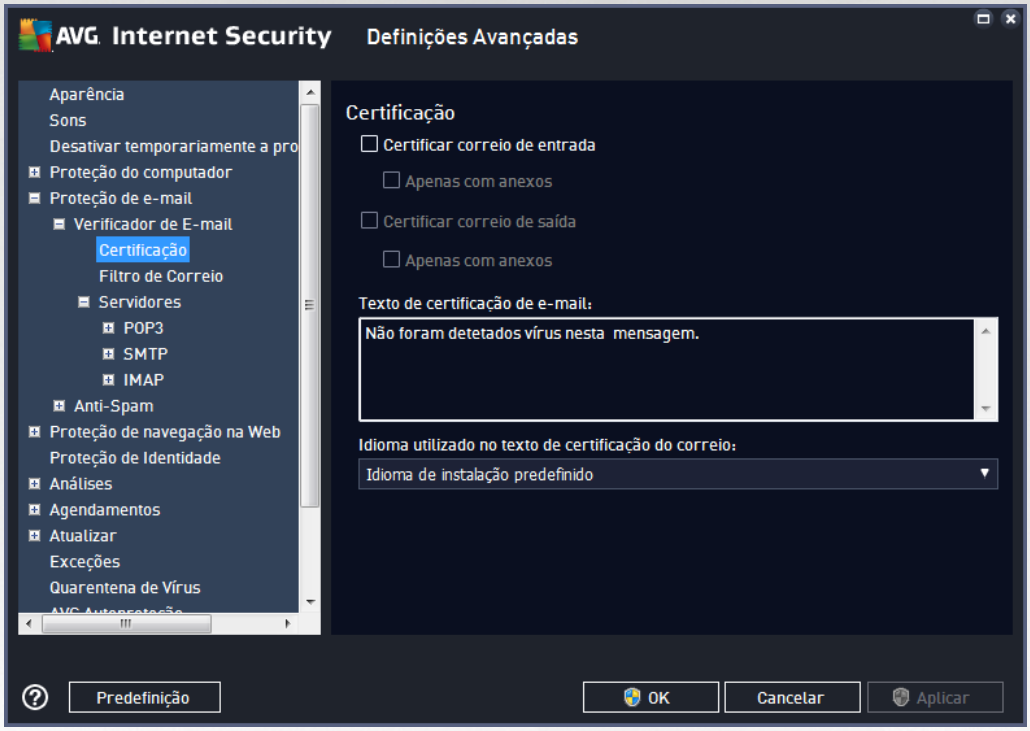
- ***Reportar ficheiros que contêm macros*** – uma macro é uma sequência predefinida de passos destinada a facilitar determinadas tarefas ao utilizador (*as macros do MS Word são amplamente conhecidas*). Como tal, uma macro pode conter instruções potencialmente perigosas e pode querer marcar a caixa para se certificar de que os ficheiros com macros serão reportados como suspeitos.

- ***Reportar extensões ocultas*** – uma extensão oculta pode fazer, por exemplo, com que um ficheiro executável suspeito "qualquercoisa.txt.exe" pareça um inofensivo ficheiro de texto "qualquercoisa.txt"; marque a caixa para reportar esses ficheiros como potencialmente perigosos.

- ***Mover anexos reportados para a Quarentena de Vírus*** – especifique se pretende ser notificado via e-mail acerca de arquivos protegidos por palavra-passe, documentos protegidos por palavra-passe,

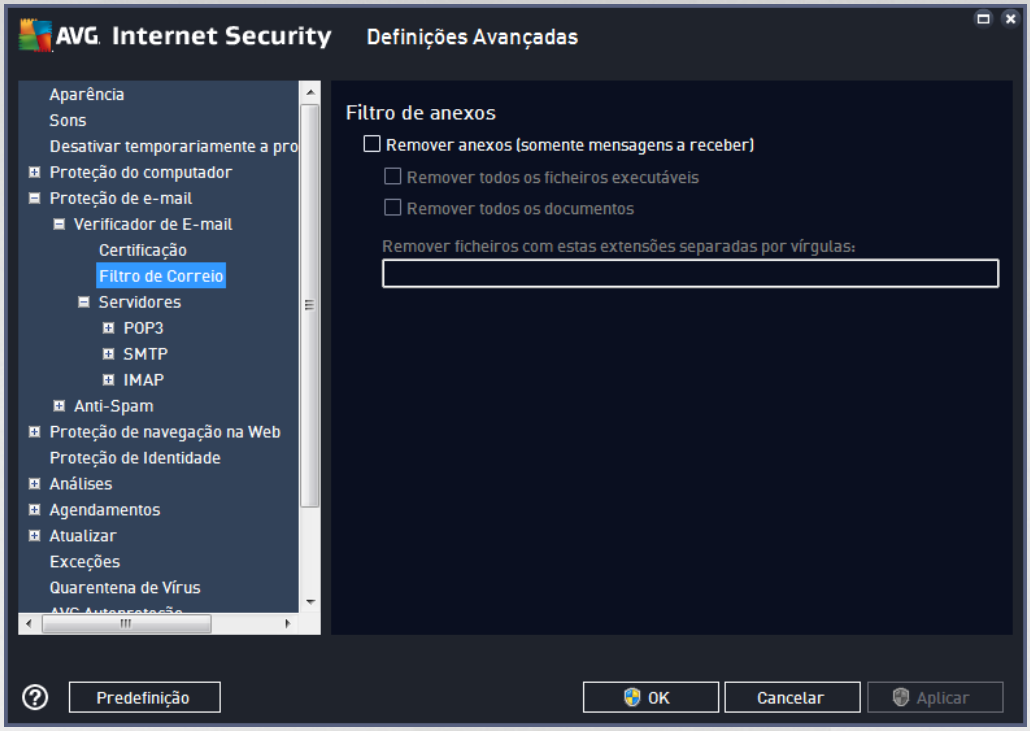
ficheiros que contêm macros e/ou ficheiros com extensões ocultas detetados como anexos das mensagens de e-mail analisadas. Se for identificada uma mensagem dessas durante a análise, defina se o objeto com infeção detetado deve ser movido para a Quarentena de Vírus.

Na janela ***Certificação*** pode marcar as caixas específicas para decidir se pretende certificar o correio a receber (***Certificar correio de entrada***) e/ou o correio a enviar (***Certificar correio de saída***). Pode ainda especificar, para cada uma destas opções, o parâmetro ***Apenas com anexos*** para que a certificação só seja adicionada a mensagens de e-mail que contenham anexos:



Por predefinição, o texto de certificação é composto por uma mera informação básica que declara que *Não foram detetados vírus nesta mensagem.* No entanto, esta informação pode ser alterada conforme as suas necessidades: escreva o texto de certificação pretendido no campo ***Texto de certificação de e-mail***. Na secção ***Idioma utilizado no texto de certificação do correio*** pode ainda definir em que idioma deverá ser apresentada a informação da certificação gerada automaticamente (*Não foram detetados vírus nesta mensagem*).

Nota: *tenha em consideração que só o texto predefinido será apresentado no idioma selecionado e que texto personalizado não será traduzido automaticamente!*



A janela ***Filtro de anexos*** permite-lhe configurar parâmetros para a análise de anexos de e-mail. A opção ***Remover anexos*** está desativada por predefinição. Se decidir ativá-la, todos os anexos das mensagens de e-mail detetados como infetados ou potencialmente perigosos serão removidos automaticamente. Se quiser definir tipos específicos de anexos que podem ser removidos, selecione a opção respetiva:

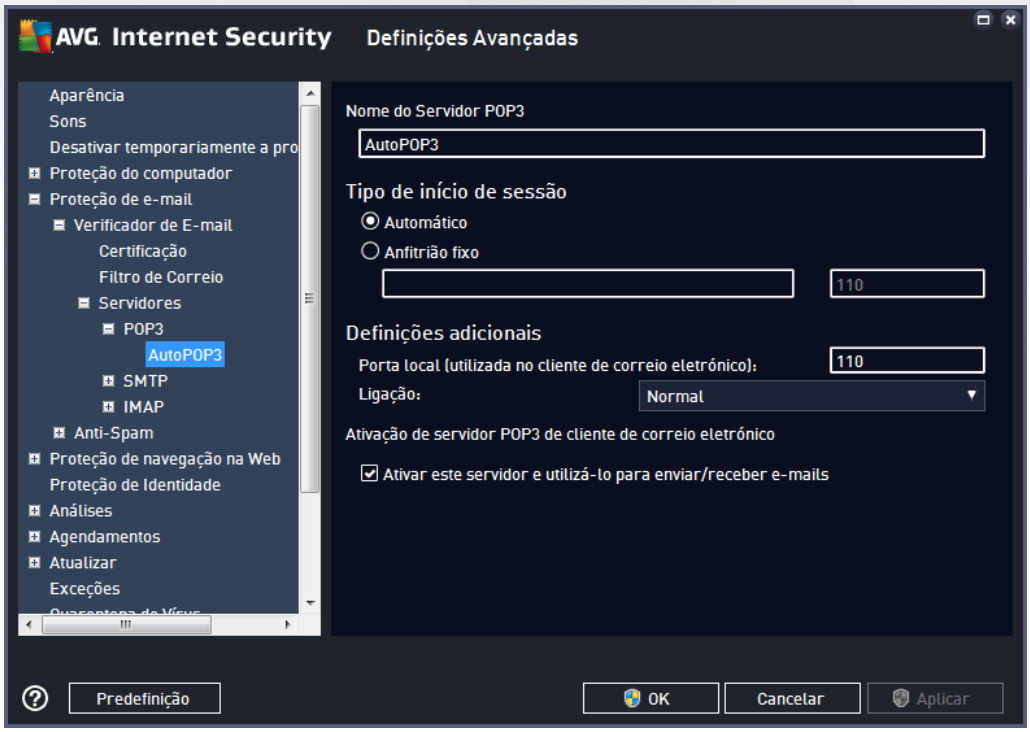
- ***Remover todos os ficheiros executáveis*** – todos os ficheiros *.exe serão eliminados
- ***Remover todos os documentos*** – todos os ficheiros *.doc, *.docx, *.xls, *.xlsx serão eliminados
- ***Remover ficheiros com estas extensões separadas por vírgulas*** – removerá todos os ficheiros com as extensões definidas

Na secção ***Servidores*** pode editar os parâmetros dos servidores do Verificador de E-mail:

- Servidor POP3
- Servidor SMTP
- Servidor IMAP

Também pode definir novos servidores para o correio de entrada e de saída, utilizando o botão ***Adicionar novo servidor***.

Nesta janela pode configurar um novo servidor do Verificador de E-mail utilizando o protocolo POP3 para e-mail a receber:

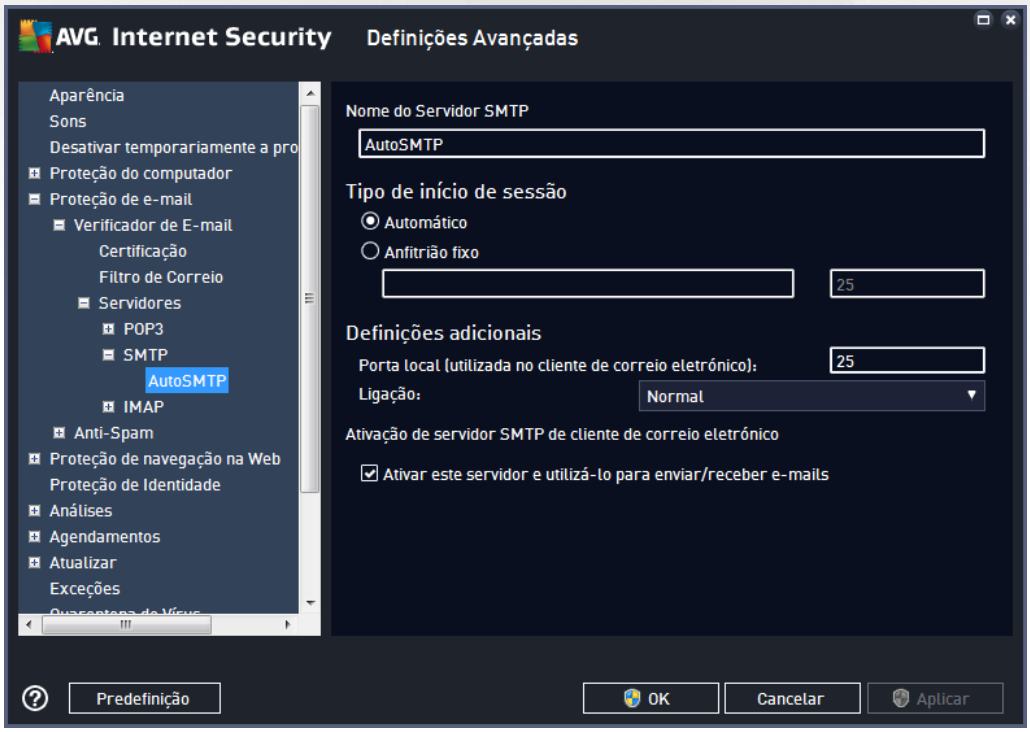


- ***Nome do Servidor POP3*** – neste campo pode especificar o nome de servidores adicionados

recentemente (*para adicionar um servidor POP3, clique com o botão direito do rato sobre o item POP3 do menu de navegação à esquerda*).

- ***Tipo de início de sessão*** – define o método para determinar o servidor de e-mail utilizado para e-mail a receber:
    - ***Automático*** – o início de sessão será realizado automaticamente, de acordo com as definições do seu cliente de e-mail.
    - ***Anfitrião fixo*** – neste caso, o programa utilizará sempre o servidor especificado aqui. Indique o endereço ou o nome do servidor de e-mail. O nome de início de sessão permanece inalterado. Para um nome, pode utilizar um nome de domínio (*por exemplo, pop.acme.com*) e um endereço IP (*por exemplo, 123.45.67.89*). Se o servidor de e-mail utilizar uma porta não padrão, pode especificar esta porta a seguir ao nome do servidor, utilizando dois pontos como delimitador (*por exemplo, pop.acme.com:8200*). A porta padrão para comunicação POP3 é 110.
- ***Definições adicionais*** – especifica parâmetros mais detalhados:
    - ***Porta local*** – especifica a porta em que a comunicação da sua aplicação de e-mail deverá ser processada. Tem de definir esta porta na sua aplicação de e-mail como sendo a porta para a comunicação POP3.
    - ***Ligação*** – no menu pendente pode especificar que tipo de ligação utilizar (*normal/SSL/SSL predefinida*). Se selecionar uma ligação SSL, os dados enviados são encriptados, não havendo o risco de serem seguidos ou controlados por terceiros. Esta funcionalidade só estará disponível se o servidor de e-mail de destino a suportar.
- ***Ativação de servidor POP3 de cliente de correio eletrónico*** – marque/desmarque este item para ativar ou desativar o servidor POP3 especificado

Nesta janela pode configurar um novo servidor do Verificador de E-mail utilizando o protocolo SMTP para e-mail a enviar:

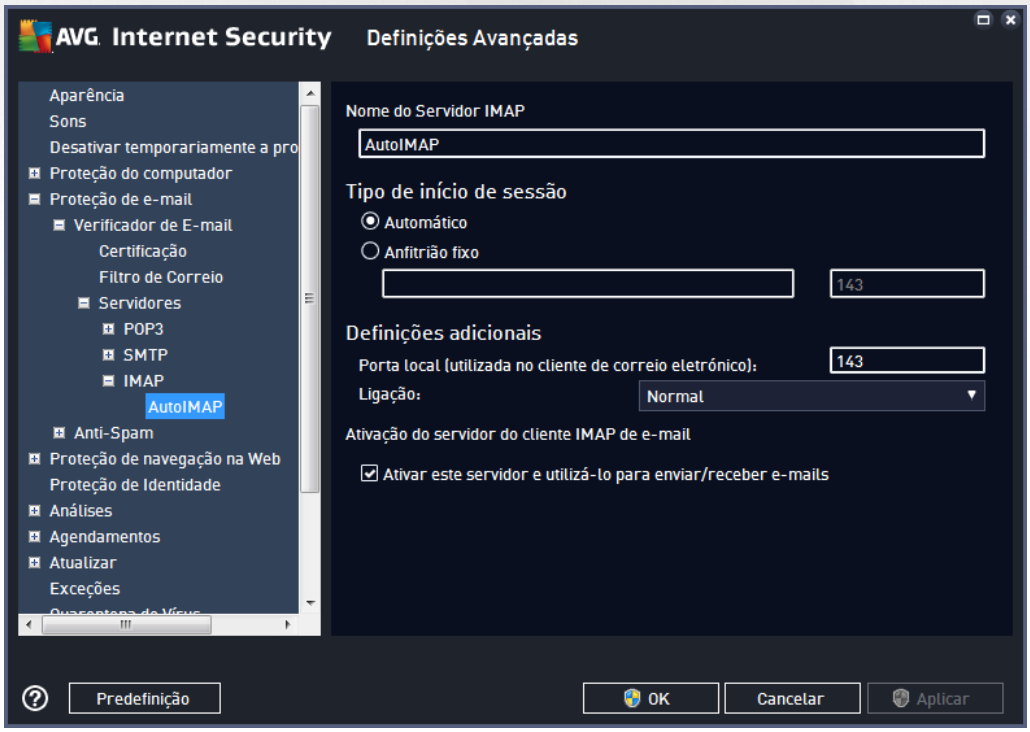


- ***Nome do Servidor SMTP*** – neste campo pode especificar o nome de servidores adicionados

recentemente (*para adicionar um servidor SMTP, clique com o botão direito do rato sobre o item SMTP do menu de navegação à esquerda*). Este campo estará desativado para servidores "AutoSMTP" criados automaticamente.

- ***Tipo de início de sessão*** – define o método para determinar o servidor de e-mail utilizado para e-mail a enviar:
    - ***Automático*** – o início de sessão será realizado automaticamente, de acordo com as definições do seu cliente de e-mail.
    - ***Anfitrião fixo*** – neste caso, o programa utilizará sempre o servidor especificado aqui. Indique o endereço ou o nome do servidor de e-mail. Pode utilizar um nome de domínio (*por exemplo, smtp.acme.com)*) e um endereço IP (*por exemplo, 123.45.67.89*) para um nome. Se o servidor de correio utilizar uma porta não padrão, pode escrever esta porta atrás do nome do servidor, utilizando dois pontos como delimitador (*por exemplo, smtp.acme.com:8200*). A porta padrão para comunicação SMTP é 25.
- ***Definições adicionais*** – especifica parâmetros mais detalhados:
    - ***Porta local*** – especifica a porta em que a comunicação da sua aplicação de e-mail deverá ser processada. Tem de definir esta porta na sua aplicação de e-mail como sendo a porta para a comunicação SMTP.
    - ***Ligação*** – neste menu pendente pode especificar que tipo de ligação utilizar (*normal/SSL/SSL predefinida*). Se selecionar uma ligação SSL, os dados enviados são encriptados, não havendo o risco de serem seguidos ou controlados por terceiros. Esta funcionalidade só está disponível se o servidor de e-mail de destino a suportar.
- ***Ativação de servidor SMTP de cliente de correio eletrónico*** – marque/desmarque esta caixa para ativar/desativar o servidor SMTP especificado acima

Nesta janela pode configurar um novo servidor do Verificador de E-mail utilizando o protocolo IMAP para e-mail a enviar:

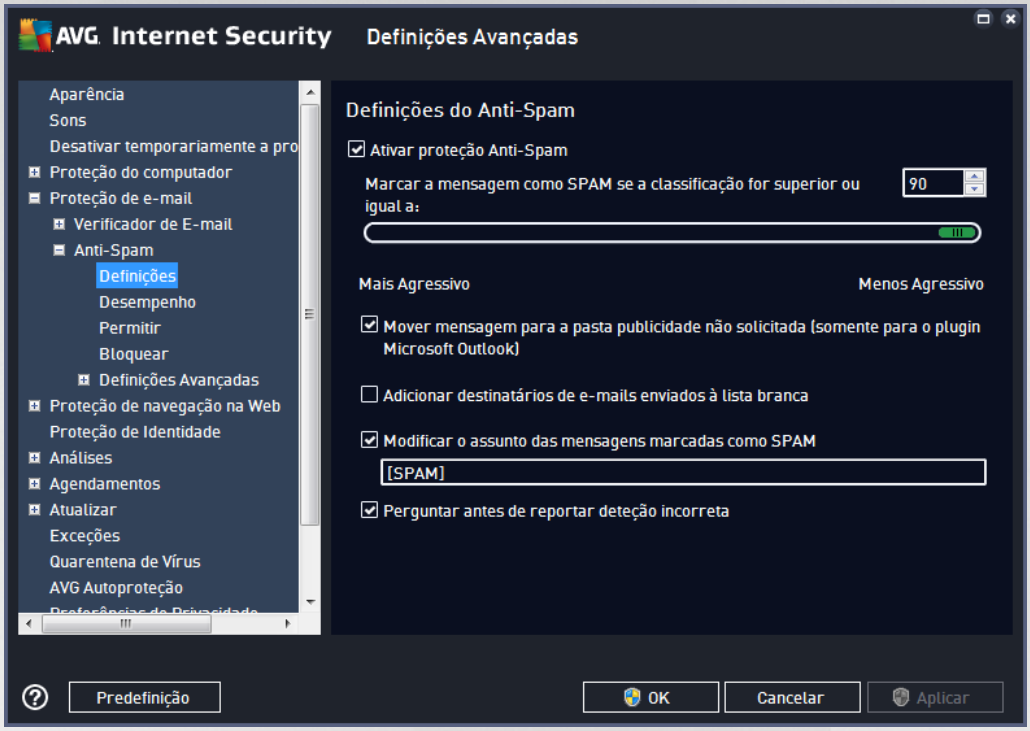


- ***Nome do Servidor IMAP*** – neste campo pode especificar o nome de servidores adicionados

recentemente (*para adicionar um servidor IMAP, clique com o botão direito do rato sobre o item IMAP do menu de navegação à esquerda*).

- ***Tipo de início de sessão*** – define o método para determinar o servidor de e-mail utilizado para e-mail a enviar:
    - ***Automático*** – o início de sessão será realizado automaticamente, de acordo com as definições do seu cliente de e-mail.
    - ***Anfitrião fixo*** – neste caso, o programa utilizará sempre o servidor especificado aqui. Indique o endereço ou o nome do servidor de e-mail. Pode utilizar um nome de domínio (*por exemplo, smtp.acme.com)*) e um endereço IP (*por exemplo, 123.45.67.89*) para um nome. Se o servidor de correio utilizar uma porta não padrão, pode escrever esta porta atrás do nome do servidor, utilizando dois pontos como delimitador (*por exemplo, imap.acme.com:8200*). A porta padrão para comunicação IMAP é a 143.
- ***Definições adicionais*** – especifica parâmetros mais detalhados:
    - ***Porta local (utilizada no cliente de correio eletrónico)*** – especifica a porta em que a comunicação da sua aplicação de e-mail deverá ser processada. Tem de definir esta porta na sua aplicação de e-mail como sendo a porta para a comunicação IMAP.
    - ***Ligação*** – neste menu pendente pode especificar que tipo de ligação utilizar (*normal/SSL/SSL predefinida*). Se selecionar uma ligação SSL, os dados enviados são encriptados, não havendo o risco de serem seguidos ou controlados por terceiros. Esta funcionalidade só está disponível se o servidor de e-mail de destino a suportar.
- ***Ativação do servidor do cliente IMAP de e-mail*** – marque/desmarque esta caixa para ativar/desativar o servidor IMAP especificado acima

7.5.2. Anti-Spam



Na janela ***Definições do Anti-Spam*** pode marcar/desmarcar a caixa ***Ativar proteção Anti-Spam*** para permitir/interditar a análise anti-spam de comunicações de e-mail. Esta opção está ativada por predefinição e, como sempre, é recomendável que mantenha esta configuração a menos que tenha uma razão válida para a alterar.

A seguir, também pode selecionar medidas de classificação mais ou menos agressivas. O filtro ***Anti-Spam*** atribui uma classificação a cada mensagem (*ou seja, o quão similar o conteúdo da mensagem é com SPAM*) baseada em várias técnicas de análise dinâmica. Pode ajustar a definição ***Marcar mensagem como spam se a pontuação for superior a*** digitando o valor ou deslocando o cursor para a esquerda ou para a direita.

O intervalo de valores permitido é de 50 a 90. Veja aqui uma revisão geral do limiar de classificação:

- ***Valor 80-90*** – as mensagens de e-mail passíveis de serem spam serão filtradas. É igualmente possível que algumas mensagens que não são spam sejam incorretamente filtradas.
- ***Valor 60-79*** – considerada uma configuração agressiva. As mensagens de e-mail suscetíveis de serem spam serão filtradas. É muito provável que sejam igualmente filtradas mensagens que não são spam.
- ***Valor 50-59*** – configuração muito agressiva. Existe uma forte probabilidade de considerar mensagens de e-mail que não são spam como sendo spam. ***Este intervalo não é recomendado para uma utilização normal.***

Na janela ***Definições do Anti-Spam*** pode definir a forma como os e-mails detetados como spam deverão ser tratados:

- ***Mover mensagem para a pasta publicidade não solicitada*** *(apenas para o plug-in Microsoft Outlook)* – marque esta caixa para especificar que cada mensagem de spam detetada deverá ser

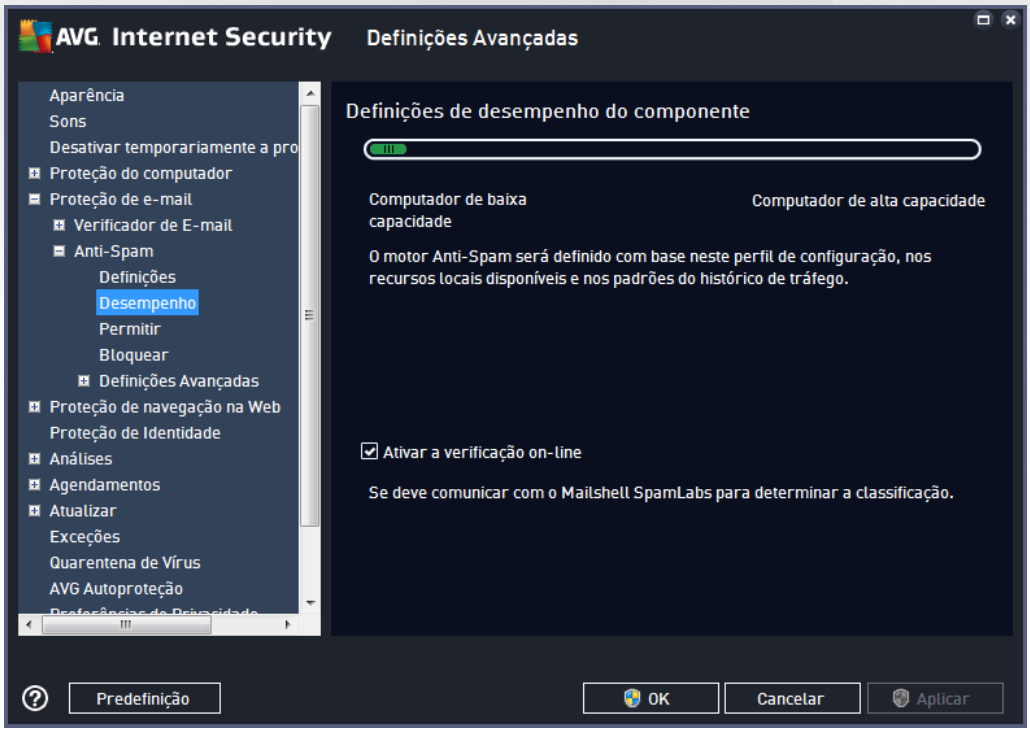
movida automaticamente para a pasta publicidade não solicitada especificada no seu cliente de e-mail MS Outlook. De momento, esta funcionalidade não é suportada noutros clientes de correio eletrónico.

- ***Adicionar destinatários de e-mails enviados à lista branca*** – assinale esta caixa para confirmar que todos os destinatários de e-mails enviados são de confiança e que todas as mensagens de e-mail enviadas das contas desses destinatários podem ser entregues.

- ***Modificar o assunto das mensagens marcadas como SPAM*** – assinale esta caixa se quiser que todas as mensagens detetadas como sendo spam sejam marcadas com uma palavra ou carácter específico no campo de assunto da mensagem; o texto pretendido pode ser digitado no campo de texto ativado.

- ***Perguntar antes de reportar deteção incorreta*** – desde que, durante o processo de instalação, tenha aceitado participar no projeto de Preferências de Privacidade. Se for o caso, permitiu a reportação de ameaças detetadas à AVG. A reportação é feita automaticamente. No entanto, pode assinalar esta caixa para confirmar que pretende ser inquirido antes da reportação de qualquer deteção de spam à AVG, para assegurar que a mensagem deverá efetivamente ser classificada como spam.

A janela ***Definições de desempenho do componente*** (*acessível através do item* ***Desempenho*** *na navegação à esquerda*) disponibiliza as definições de desempenho do componente ***Anti-Spam***:



Desloque o cursor para a esquerda ou para a direita para alterar o nível de desempenho de análise estabelecido entre ***Computador de baixa capacidade*** / ***Computador de alta capacidade***.

- ***Computador de baixa capacidade*** – não serão utilizadas quaisquer regras durante o processo de análise para identificar spam. Serão utilizados apenas dados de aprendizagem para identificação.

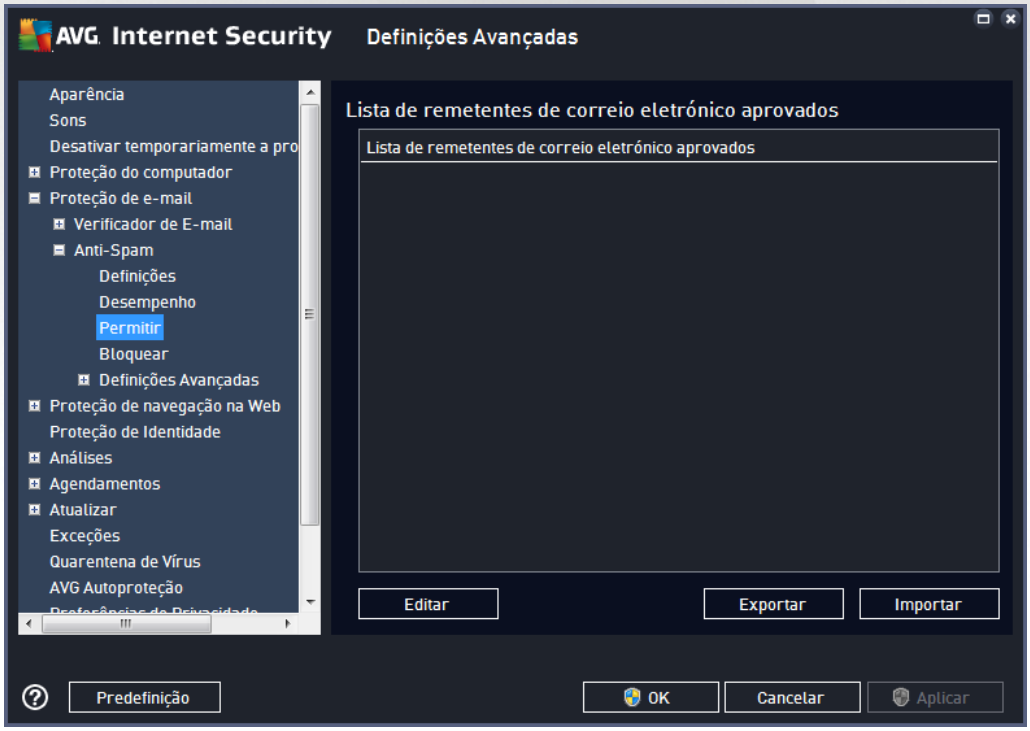
Este modo não é recomendado para uso comum, a não ser que o hardware do computador seja muito fraco.

- ***Computador de alta capacidade*** – este modo consome uma grande quantidade de memória. Durante o processo de análise para identificar spam, serão utilizadas as seguintes características: regras e cache de base de dados de spam, regras básicas e avançadas, endereços IP de remetentes de spam e bases de dados de remetentes de spam.

O item ***Ativar a verificação online*** está ativado por predefinição. Resulta numa deteção de spam mais precisa através da comunicação com os servidores Mailshell, ou seja, os dados analisados serão comparados com as bases de dados online Mailshell.

Normalmente é recomendável que mantenha as definições predefinidas e só as altere se tiver uma razão válida para o fazer. Quaisquer alterações à configuração devem ser efetuadas exclusivamente por utilizadores avançados!

O item ***Lista Branca*** abre uma janela apelidada de ***Lista de remetentes de correio eletrónico aprovados*** com uma listagem global de endereços de e-mail e de nomes de domínios aprovados cujas mensagens nunca serão assinaladas como spam.



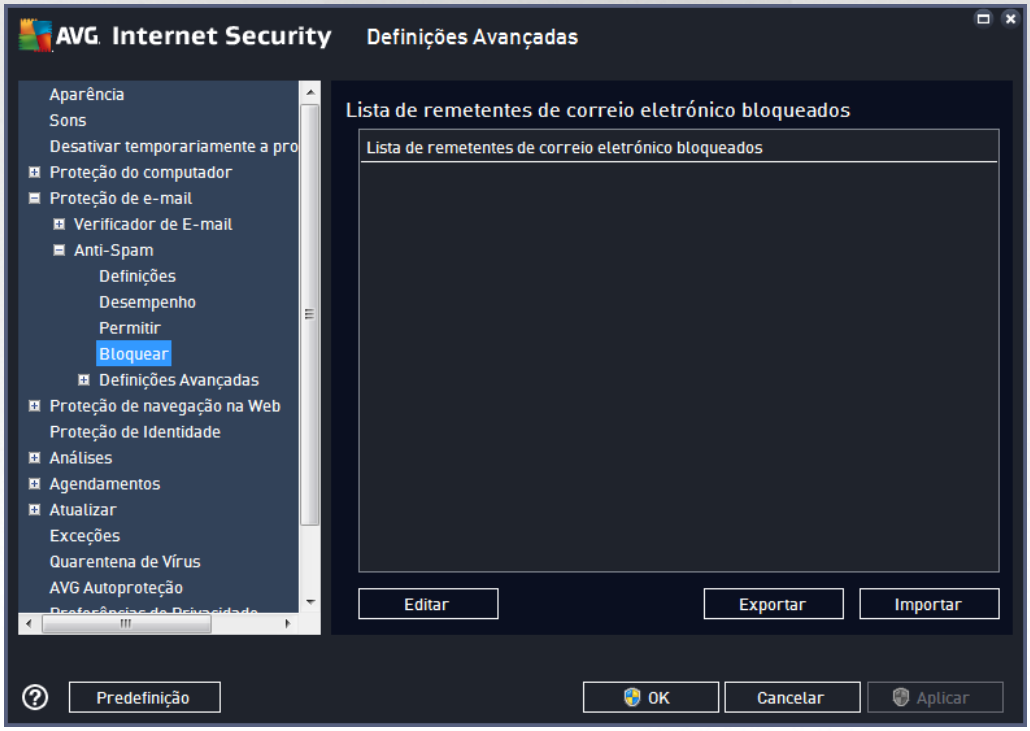
Na interface de edição pode compilar uma lista de remetentes dos quais nunca espera receber mensagens indesejadas (spam). Pode ainda compilar uma lista de nomes de domínios completos (*ex. avg.com*, que sabe que não geram spam. Quando já tiver uma lista de remetentes e/ou nomes de domínio preparada, pode introduzi-los por meio de um dos seguintes métodos: introduzindo diretamente cada endereço de correio eletrónico ou importando toda a lista de endereços de uma vez.

Botões de controlo

Estão disponíveis os seguintes botões de controlo:

- ***Editar*** – clique neste botão para abrir uma janela onde pode inserir manualmente uma lista de endereços (*também pode utilizar o método copiar e colar*). Insira um item (*remetente, nome de domínio*) por linha.
- ***Exportar*** – se decidir exportar os registos para uma determinada finalidade, pode fazê-lo clicando neste botão. Todos os registos serão guardados num ficheiro de texto simples.
- ***Importar*** – se já tiver um ficheiro de texto preparado com endereços de e-mail/nomes de domínios, pode simplesmente importá-lo, selecionando este botão. O conteúdo do ficheiro deve conter apenas um item (*endereço, nome de domínio*) por linha.

O item ***Lista Negra*** abre uma janela com uma lista global de endereços de e-mail e de nomes de domínios bloqueados cujas mensagens serão sempre assinaladas como spam.



Na interface de edição pode compilar uma lista de remetentes dos quais espera receber mensagens indesejadas (*spam*). Pode ainda compilar uma lista de nomes de domínios completos (*ex. spammingcompany.com*, dos quais recebe ou espera receber mensagens de spam. Todas as mensagens de e-mail dos endereços/domínios listados serão identificadas como spam. Quando já tiver uma lista de remetentes e/ou nomes de domínios preparada, pode introduzi-los por meio de um dos seguintes métodos: introduzindo diretamente cada endereço de e-mail ou importando toda a lista de endereços de uma vez.

Botões de controlo

Estão disponíveis os seguintes botões de controlo:

- ***Editar*** – clique neste botão para abrir uma janela onde pode inserir manualmente uma lista de endereços (*também pode utilizar o método copiar e colar*). Insira um item (*remetente, nome de domínio*) por linha.

- ***Exportar*** – se decidir exportar os registos para uma determinada finalidade, pode fazê-lo clicando neste botão. Todos os registos serão guardados num ficheiro de texto simples.

- ***Importar*** – se já tiver um ficheiro de texto preparado com endereços de e-mail/nomes de domínios, pode simplesmente importá-lo, selecionando este botão.

O separador Definições Avançadas contém opções de definições suplementares para a funcionalidade Anti-Spam. Estas definições destinam-se exclusivamente a utilizadores experientes, regra geral administradores de redes que precisem de configurar detalhadamente a proteção anti-spam para uma proteção superior dos servidores de e-mail. Como tal, não existe qualquer ajuda suplementar disponível para as janelas individuais; no entanto, está disponível uma pequena descrição de cada opção diretamente na interface do utilizador. Recomendamos vivamente que não altere quaisquer definições a menos que esteja perfeitamente familiarizado com as definições avançadas do Spamcatcher (MailShell Inc.). Quaisquer alterações inadequadas podem resultar numa diminuição de desempenho ou num mau funcionamento do componente.

Se contudo necessitar imperativamente de alterar a configuração do componente Anti-Spam nos módulos mais avançados, por favor siga as instruções facultadas na interface do utilizador. De um modo geral, encontrará em cada janela uma única funcionalidade específica que pode editar. A descrição da funcionalidade está sempre incluída na janela propriamente dita. Pode editar os seguintes parâmetros:

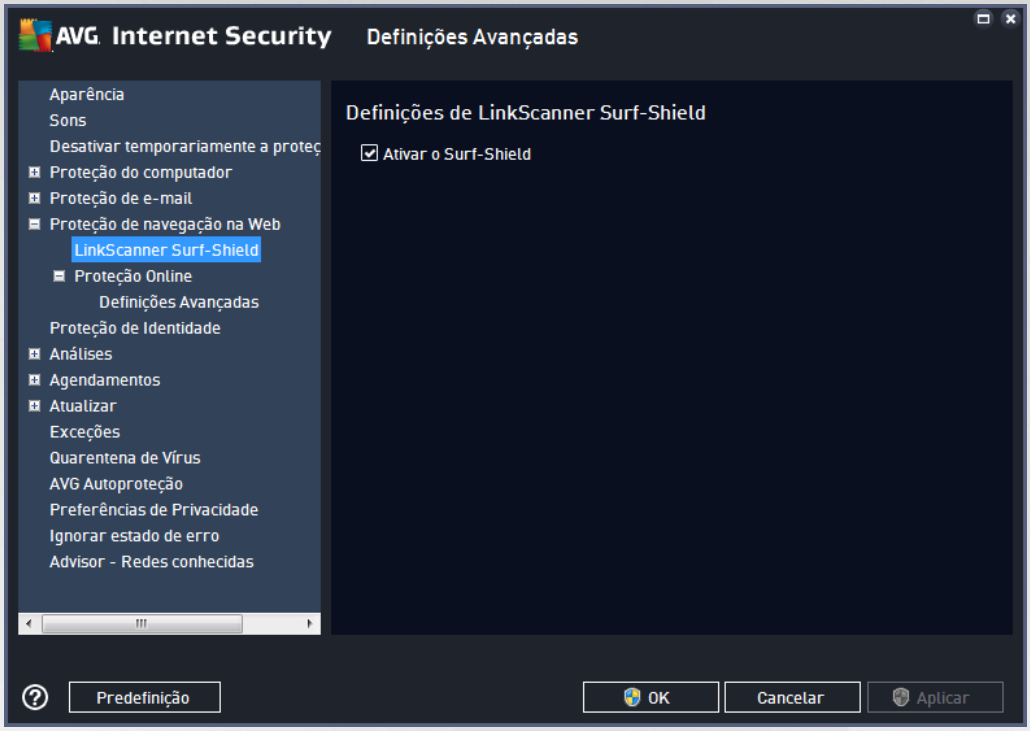
- ***Filtragem*** – lista de idiomas, lista de países, IPs aprovados, IPs bloqueados, países bloqueados, conjuntos de caracteres bloqueados, remetentes falsificados

- ***RBL*** – servidores RBL, multicorrespondências, limiar, tempo limite, máximo de IPs

- ***Ligação à Internet*** – tempo limite, servidor proxy, autenticação de servidor proxy

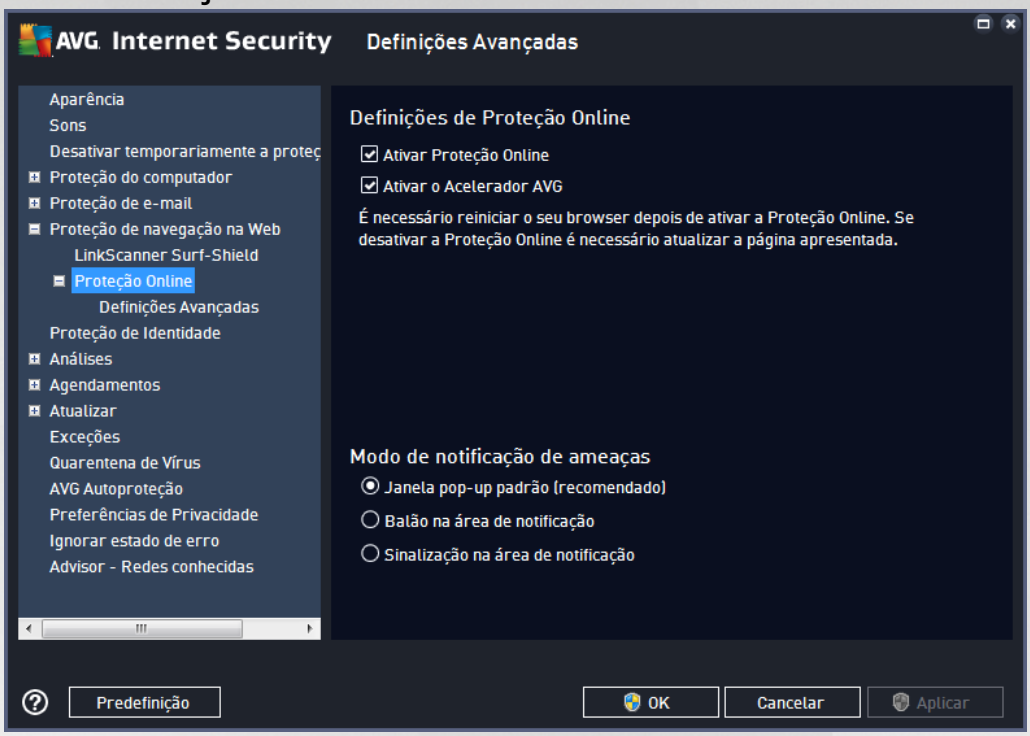
7.6. Proteção de navegação na Web

A janela ***Definições do LinkScanner*** permite marcar/desmarcar as seguintes funcionalidades:



- ***Ativar o Surf-Shield*** – (*ativado por predefinição*): proteção ativa (*em tempo real*) contra websites maliciosos à medida que estes são visitados. Ligações de websites maliciosos conhecidos são bloqueadas à medida que são acedidas pelo utilizador através de um browser Web (*ou qualquer outra aplicação que utilize HTTP*).

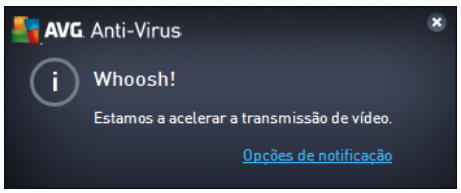
7.6.1. Proteção Online



A janela ***Proteção Online*** apresenta as seguintes opções:

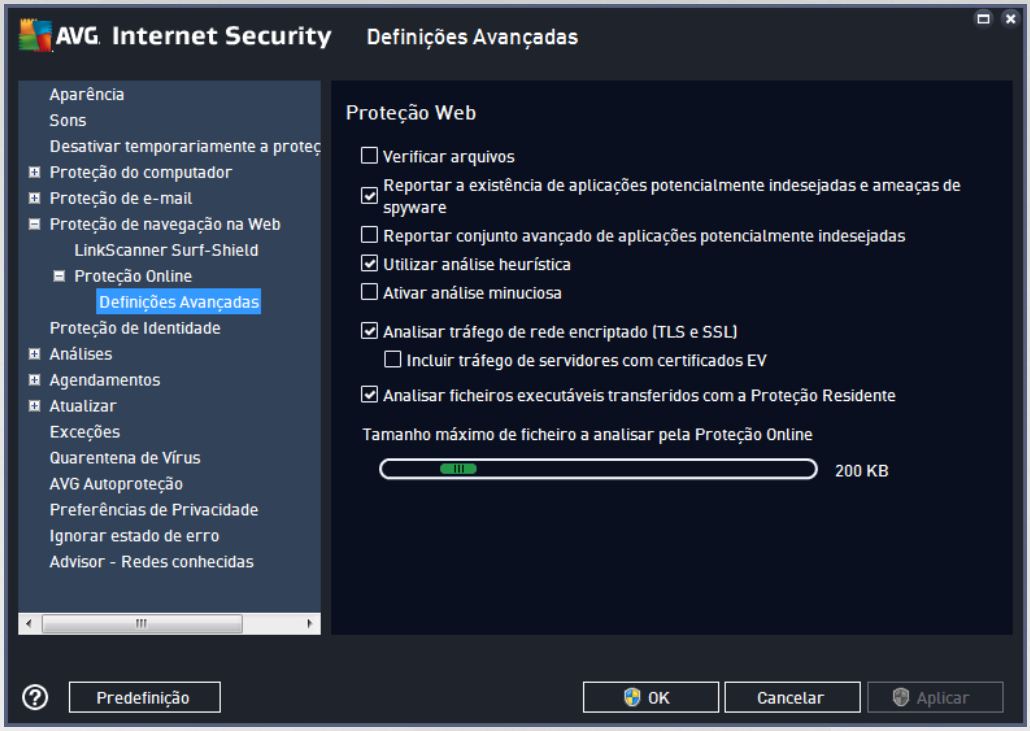
- ***Ativar a Proteção Online*** *(ativado por predefinição)* – Ativar/desativar por completo o serviço ***Proteção Online***. Para definições avançadas da ***Proteção Online***, continue para a janela seguinte intitulada Proteção Web.

- ***Ativar o Acelerador AVG*** *(ativado por predefinição)* – Ativar/desativar o serviço Acelerador AVG. O Acelerador AVG permite uma reprodução de vídeos online mais fluida e facilita as transferências. Quando o processo de aceleração do vídeo estiver em curso, será notificado via uma janela de notificação na barra de tarefas:



Modo de notificação de ameaças

Na parte inferior da janela, selecione de que forma pretende ser informado de possíveis ameaças detetadas: através de uma janela pop-up padrão, através de um balão na área de notificação ou através de sinalização na área de notificação.



Na janela ***Proteção Web*** pode editar a configuração do componente em relação à análise do conteúdo de websites. A interface de edição permite-lhe configurar as seguintes opções elementares:

- ***Verificar arquivos*** (*desativado por predefinição*): analisar o conteúdo de arquivos possivelmente incluídos na página www a ser apresentada.
- ***Reportar aplicações potencialmente indesejadas e ameaças de spyware*** (*ativado por predefinição*): marque esta opção para ativar a análise que procura spyware e também vírus. O Spyware representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade ativada, uma vez que aumenta a segurança do seu computador.
- ***Reportar conjunto avançado de aplicações potencialmente indesejadas*** (*desativado por predefinição*): marque esta opção para detetar pacotes expandidos de spyware: programas que são perfeitamente fidedignos e inofensivos quando adquiridos diretamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, poderá bloquear programas legais e está, como tal, desativada por predefinição.
- ***Utilizar análise heurística*** (*ativado por predefinição*): analisar o conteúdo da página a ser apresentada utilizando o método de análise heurística (*emulação dinâmica das instruções do objeto analisado num ambiente de computador virtual*).
- ***Ativar análise minuciosa*** (*desativado por predefinição*): em situações específicas (*suspeitas de infeção do computador*) pode marcar esta opção para ativar os algoritmos de análise mais rigorosos que irão analisar todas as áreas do seu computador, incluindo as que raramente são infetadas, por precaução. Tenha em consideração que este método é bastante demorado.

- ***Analisar tráfego de rede encriptado (TLS e SSL)*** (*ativado por predefinição*): deixe esta opção marcada para permitir que o AVG analise também comunicação em rede encriptada, ou seja, ligações estabelecidas através de protocolos de segurança (SSL e TLS, a versão mais recente do protocolo). Aplica-se a sites que utilizam HTTPS e ligações de clientes de e-mail que utilizam TLS/SSL. O tráfego seguro é desencriptado, analisado para procurar malware e encriptado novamente para chegar em segurança ao seu computador. Dentro desta opção, pode escolher ***Incluir tráfego de servidores com certificados EV*** para analisar também comunicação em rede encriptada de servidores com certificado de validação avançada (EV – Extended Validation). A emissão de um certificado EV necessita de validação abrangente por parte da autoridade de certificação; por conseguinte, os sites que utilizam o certificado são muito mais fidedignos *(com menor probabilidade de distribuição de malware)*. Por esse motivo, pode optar por não analisar tráfego de servidores com certificado EV, o que tornará a comunicação encriptada moderadamente mais rápida.

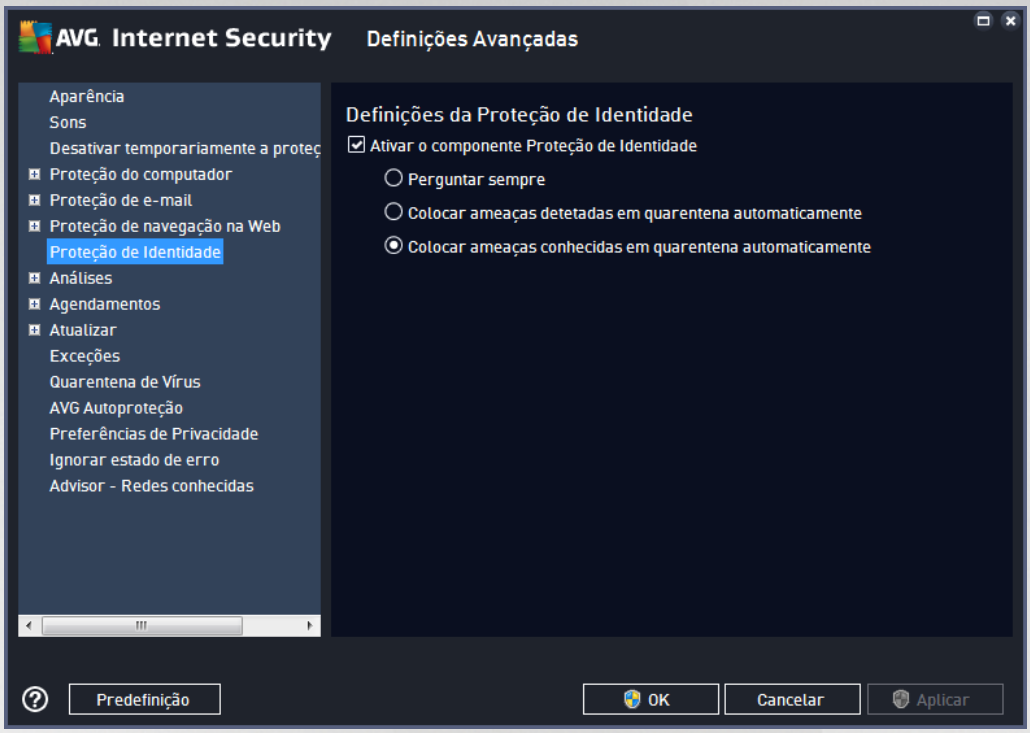
- ***Analisar ficheiros executáveis transferidos com a Proteção Residente*** (*ativado por predefinição*): analisar ficheiros executáveis *(normalmente, ficheiros com extensões .exe, .bat, .com)* depois de serem transferidos. A Proteção Residente analisa os ficheiros antes de serem transferidos para assegurar que não entra código malicioso no computador. No entanto, essa análise é limitada pelo ***Tamanho máximo por parte do ficheiro a analisar*** – ver o item seguinte nesta janela. Por conseguinte, os ficheiros grandes são analisados parte a parte, o que também acontece com a maioria dos ficheiros executáveis. Os ficheiros executáveis podem realizar várias tarefas no computador e é essencial que sejam 100% seguros. É possível garantir essa segurança analisando o ficheiro por partes antes de ser transferido e imediatamente após a conclusão da transferência. É aconselhável manter esta opção marcada. Se desativar esta opção, poderá ter à mesma a certeza de que o AVG continuará a encontrar códigos possivelmente perigosos. O que poderá acontecer por vezes é o programa não conseguir avaliar um ficheiro executável como um ficheiro complexo, o que poderá originar alguns falsos positivos.

O cursor existente na janela permite definir o ***Tamanho máximo por parte do ficheiro a analisar*** – se os ficheiros incluídos estiverem presentes na página apresentada, também pode analisar o conteúdo dos ficheiros antes de serem transferidos para o computador. No entanto, analisar um ficheiro grande demora algum tempo e a transferência da página Web pode ser abrandada significativamente. Pode utilizar o cursor para especificar o tamanho máximo de um ficheiro que esteja para ser analisado pela ***Proteção Online***. Mesmo que o ficheiro transferido seja superior ao tamanho especificado e, como tal, não será analisado com a Proteção Online, ainda está protegido: na eventualidade de o ficheiro estar infetado, a ***Proteção Residente*** detetará o ficheiro imediatamente.

7.7. Proteção de Identidade

A ***Proteção de Identidade*** é um componente anti-malware que o protege de todos os tipos de malware (*spyware, bots, roubos de identidade, etc.*) utilizando tecnologias comportamentais e proporciona proteção imediata contra novos vírus *(para ver uma descrição detalhada da funcionalidade do componente, consulte o capítulo Identidade)*.

A janela ***Definições da Proteção de Identidade*** permite-lhe ativar/desativar as funcionalidades elementares do componente Proteção de Identidade:



Ativar o componente Proteção de Identidade (*ativado por predefinição*) – desmarque para desativar o componente Identidade. ***Recomendamos vivamente que não faça isto a menos que seja indispensável!*** Quando a Proteção de Identidade está ativada, pode especificar que ação tomar quando uma ameaça é detetada:

- ***Perguntar sempre*** – quando uma ameaça for detetada, ser-lhe-á solicitado que decida se a mesma deve ser movida para a quarentena para garantir que não são removidas aplicações que pretende ter em execução.
- ***Colocar ameaças detetadas em quarentena automaticamente*** – marque esta caixa para especificar que pretende mover todas as ameaças eventualmente detetadas para o espaço seguro da Quarentena de Vírus imediatamente. Se mantiver as predefinições, quando uma ameaça for detetada, ser-lhe-á solicitado que decida se a mesma deve ser movida para a quarentena para garantir que não são removidas aplicações que pretende ter em execução.
- ***Colocar ameaças conhecidas em quarentena automaticamente*** (*ativado por predefinição*) – mantenha este item marcado se quiser que todas as aplicações detetadas como potencial malware sejam automática e imediatamente movidas para a Quarentena de Vírus.

7.8. Análises

As definições avançadas de análise estão divididas em quatro categorias que se referem a tipos específicos de análises conforme definidas pelo fornecedor do software:

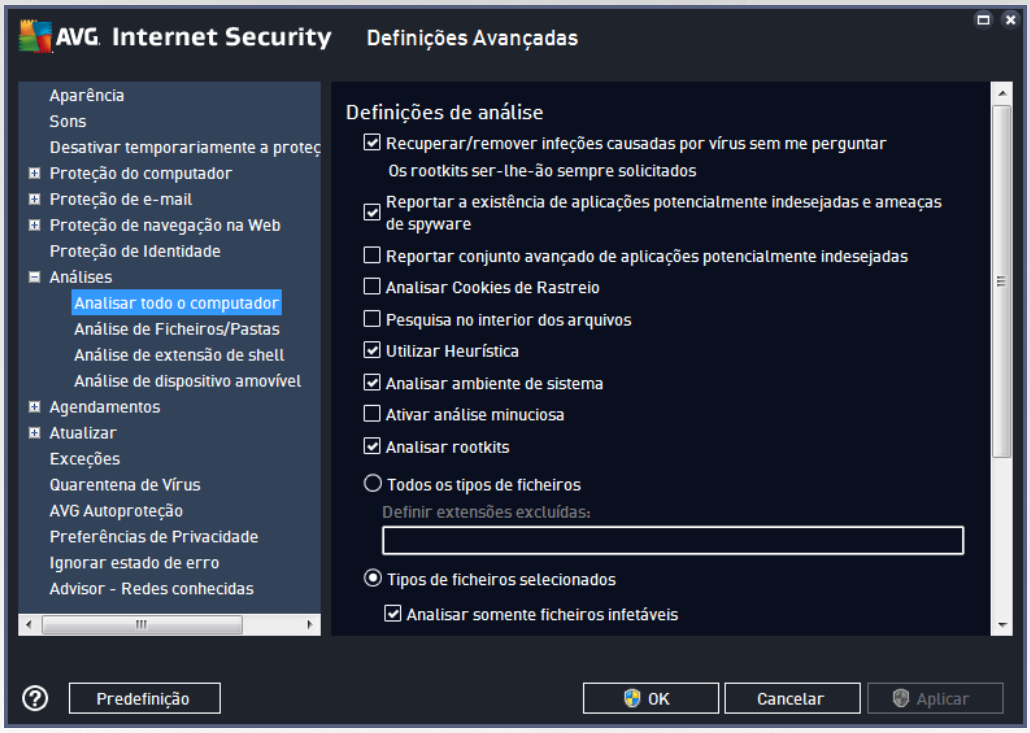
- Analisar todo o computador – análise padrão predefinida de todo o computador
- Análise de Ficheiros/Pastas – análise padrão predefinida de áreas selecionadas do seu computador
- Análise de extensão de shell – análise específica de um objeto selecionado diretamente no ambiente

do Explorador do Windows

- Análise de dispositivo amovível – análise específica de dispositivos amovíveis conectados ao seu computador

7.8.1. Analisar todo o computador

A opção ***Analisar todo o computador*** permite-lhe editar os parâmetros de uma das análises predefinidas pelo fornecedor do software, Analisar todo o computador:



Definições de análise

A secção ***Definições de análise*** disponibiliza uma lista de parâmetros de análise que podem ser opcionalmente ativados/desativados:

- ***Recuperar/remover infeções causadas por vírus sem me perguntar*** (*ativado por predefinição*) – se um vírus for detetado durante a análise, pode ser recuperado automaticamente se houver uma cura disponível. Se não for possível recuperar o ficheiro infetado automaticamente, o objeto infetado será movido para a Quarentena de Vírus.

- ***Reportar aplicações potencialmente indesejadas e ameaças de spyware*** (*ativado por predefinição*) – marque esta opção para ativar a análise que procura spyware e também vírus. O Spyware representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade ativada, uma vez que aumenta a segurança do seu computador.

- ***Reportar conjunto avançado de aplicações potencialmente indesejadas*** (*desativado por predefinição*) – marque esta opção para detetar pacotes expandidos de spyware: programas que são

perfeitamente fidedignos e inofensivos quando adquiridos diretamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, poderá bloquear programas legais e está, como tal, desativada por predefinição.

- ***Analisar Cookies de Rastreio*** (*desativado por predefinição*) – este parâmetro indica que os cookies deverão ser detetados (*os cookies HTTP são utilizados para autenticação, rastreio e manutenção de informação especifica dos utilizadores, tal como preferências de sites ou os conteúdos dos carrinhos de compras eletrónicos dos mesmos*).

- ***Pesquisa no interior dos arquivos*** (*desativado por predefinição*) – este parâmetro define que a análise deve verificar todos os ficheiros guardados em arquivos, ex.: ZIP, RAR, etc.

- ***Utilizar Heurística*** (*ativado por predefinição*) – a análise heurística (*emulação dinâmica das instruções do objeto analisado num ambiente de computador virtual*) será um dos métodos utilizados para a deteção de vírus durante a análise.

- ***Analisar ambiente de sistema*** (*ativado por predefinição*) – a análise verificará também as áreas de sistema do seu computador.

- ***Ativar análise minuciosa*** (*desativado por predefinição*) – em situações específicas (*suspeitas de infeção do computador*) pode marcar esta opção para ativar os algoritmos de análise mais rigorosos que irão analisar todas as áreas do seu computador, incluindo as que raramente são infetadas, por precaução. Tenha em consideração que este método é bastante demorado.

- ***Analisar rootkits*** (*ativado por predefinição*) – a análise Anti-Rootkit analisa o PC para procurar possíveis rootkits, ou seja, programas e tecnologias que podem ocultar atividade de malware no computador. Se for detetado um rootkit, isto não significa necessariamente que o computador esteja infetado. Em alguns casos, podem ser erroneamente detetados controladores específicos ou secções de aplicações seguras como sendo rootkits.

Também deve decidir se pretende analisar:

- ***Todos os tipos de ficheiros*** com a opção de definir exceções da análise ao indicar uma lista de extensões separadas por vírgula (*uma vez guardadas, as vírgulas mudam para ponto e vírgula*) que não devem ser analisadas.

- ***Tipos de ficheiros selecionados*** – pode especificar que pretende analisar apenas ficheiros que possam ser infetados (*ficheiros que não possam ser infetados não serão analisados, por exemplo, alguns ficheiros de texto simples ou outros ficheiros não executáveis*), incluindo ficheiros multimédia (*ficheiros de áudio, vídeo – se deixar esta caixa desmarcada, reduzirá o tempo de análise ainda mais, uma vez que os ficheiros são por vezes muito grandes e é pouco provável que estejam infetados por vírus*). Mais uma vez, pode especificar por extensões os ficheiros que deverão ser sempre analisados.

- Opcionalmente, pode decidir se pretende ***Analisar ficheiros sem extensão*** – esta opção está ativada por predefinição e é recomendável que a mantenha assim a menos que tenha uma razão válida para a alterar. Os ficheiros sem extensões são bastante suspeitos e devem ser sempre analisados.

Ajustar a rapidez de conclusão de uma Análise

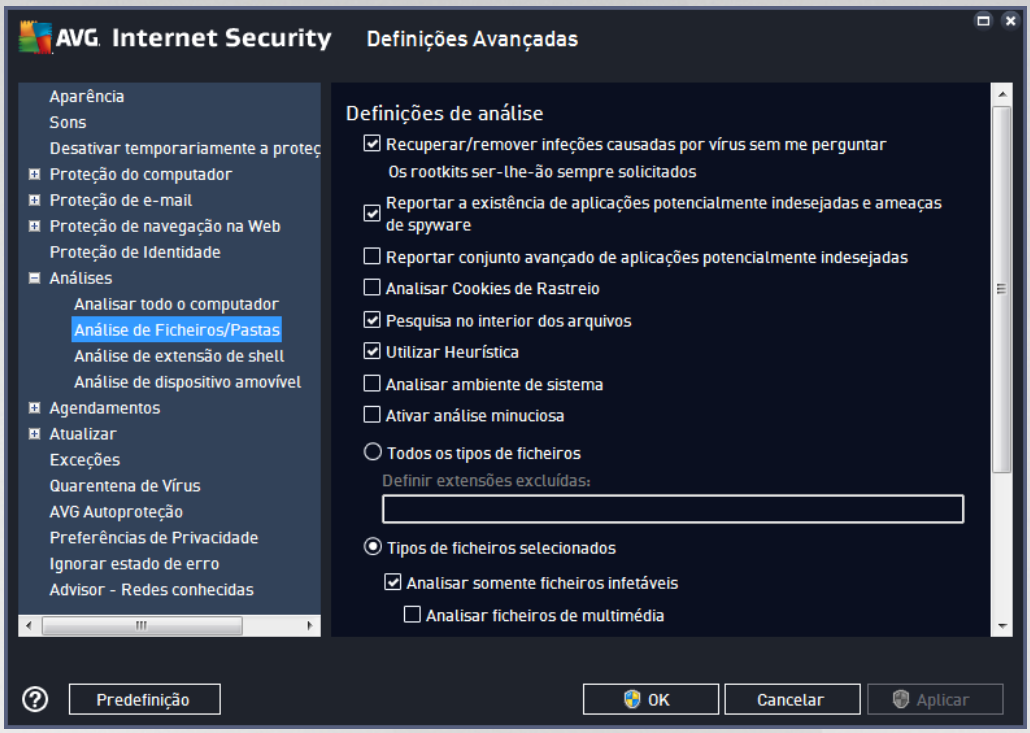
Na secção ***Ajustar a rapidez de conclusão de uma Análise*** pode ainda especificar a velocidade de análise pretendida consoante a utilização dos recursos do sistema. Por predefinição, o valor desta opção está definido para o nível de *Opção do utilizador* de utilização automática de recursos. Se quiser que a análise seja executada mais rapidamente, esta demorará menos tempo, mas os recursos do sistema utilizados aumentarão significativamente durante a execução da análise e tal diminuirá o desempenho de outras atividades no PC (*esta opção pode ser utilizada quando o seu computador estiver ligado e ninguém o estiver a utilizar*). Por outro lado, pode diminuir os recursos do sistema utilizados prolongando a duração da análise.

Definir relatórios de análise adicionais...

Clique na ligação ***Definir relatórios de análise adicionais...*** para abrir uma janela independente intitulada ***Relatórios de análise***, na qual pode selecionar vários itens para definir quais as deteções que deverão ser reportadas:

7.8.2. Análise de Ficheiros/Pastas

A interface de edição de ***Analisar pastas ou ficheiros*** é praticamente igual à janela de edição de Analisar todo o computador; no entanto, as predefinições são mais rígidas para a operação Analisar todo o computador:

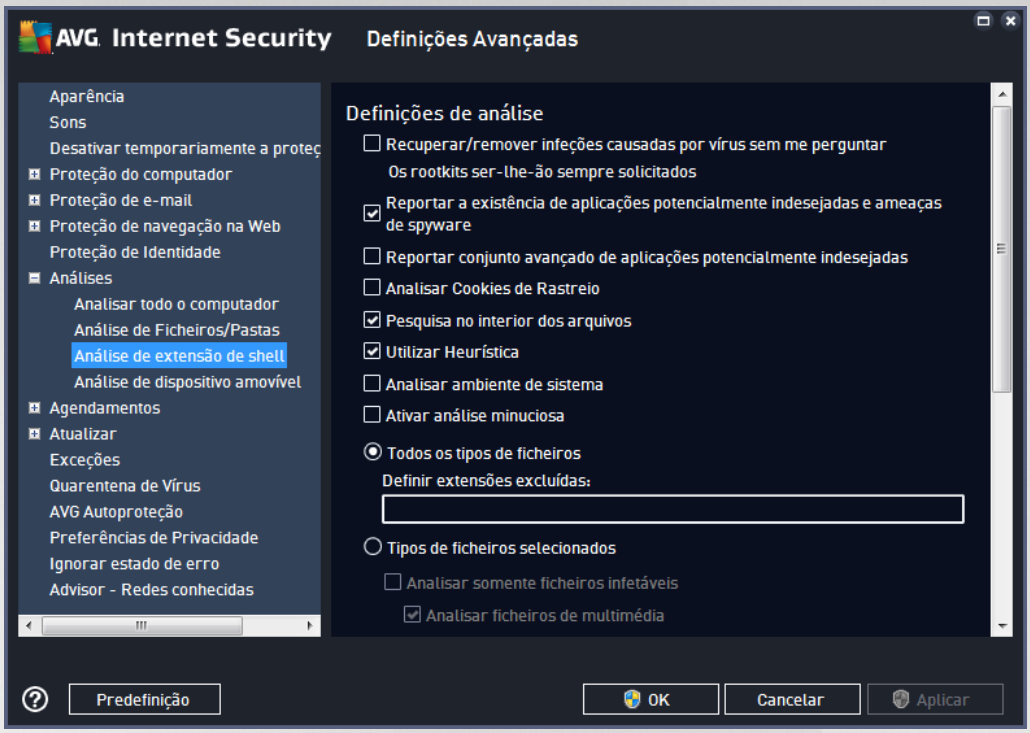


Todos os parâmetros definidos nesta janela de configuração aplicam-se apenas às áreas selecionadas para análise com Analisar pastas ou ficheiros!

Nota: *para uma descrição de parâmetros específicos, consulte o capítulo Definições Avançadas do AVG / Análises / Analisar todo o computador.*

7.8.3. Análise de extensão de shell

À semelhança do item anterior, Analisar todo o computador, o item ***Análise de extensão de shell*** também disponibiliza várias opções para edição da análise predefinida pelo fornecedor do software. Desta vez a configuração está relacionada com a análise de objetos específicos executada diretamente a partir do ambiente do Explorador do Windows (*extensão de shell*), consulte o capítulo Analisar no Explorador do Windows:



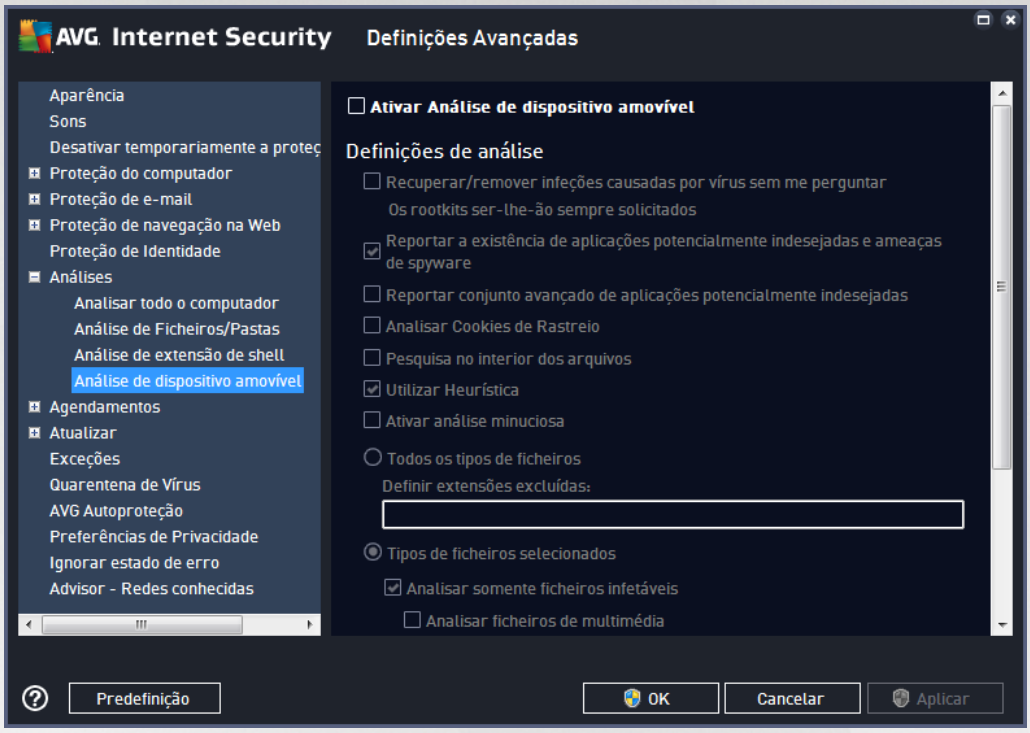
As opções de edição são praticamente iguais às que estão disponíveis para a operação Analisar todo o computador; no entanto, as predefinições são diferentes (*por exemplo, Analisar todo o computador não verifica os arquivos por predefinição, mas analisa o ambiente do sistema; com a Análise de extensão de shell verifica-se o oposto*).

Nota: *para uma descrição de parâmetros específicos, consulte o capítulo Definições Avançadas do AVG / Análises / Analisar todo o computador.*

Em comparação com a janela Analisar todo o computador, a janela ***Análise de extensão de shell*** também inclui a secção ***Visualização do progresso e dos resultados de uma análise***, na qual pode especificar se pretende que o progresso e os resultados da análise sejam acessíveis a partir da interface de utilizador do AVG. Também pode especificar que o resultado da análise só deve ser apresentado na eventualidade da deteção de uma infeção durante a análise.

7.8.4. Análise de Dispositivo Amovível

A interface de edição da ***Análise de dispositivo amovível*** também é muito semelhante à janela de edição de Analisar todo o computador:



A ***Análise de dispositivo amovível*** é iniciada automaticamente quando um dispositivo amovível é ligado ao seu computador. Por predefinição, esta análise está desativada. No entanto, é crucial que seja efetuada a análise de dispositivos amovíveis por potenciais ameaças uma vez que estes são das maiores fontes de infeção. Para que esta análise esteja pronta e seja iniciada automaticamente quando necessário, selecione a opção ***Ativar Análise de dispositivo amovível***.

Nota: *para uma descrição de parâmetros específicos, consulte o capítulo Definições Avançadas do AVG / Análises / Analisar todo o computador.*

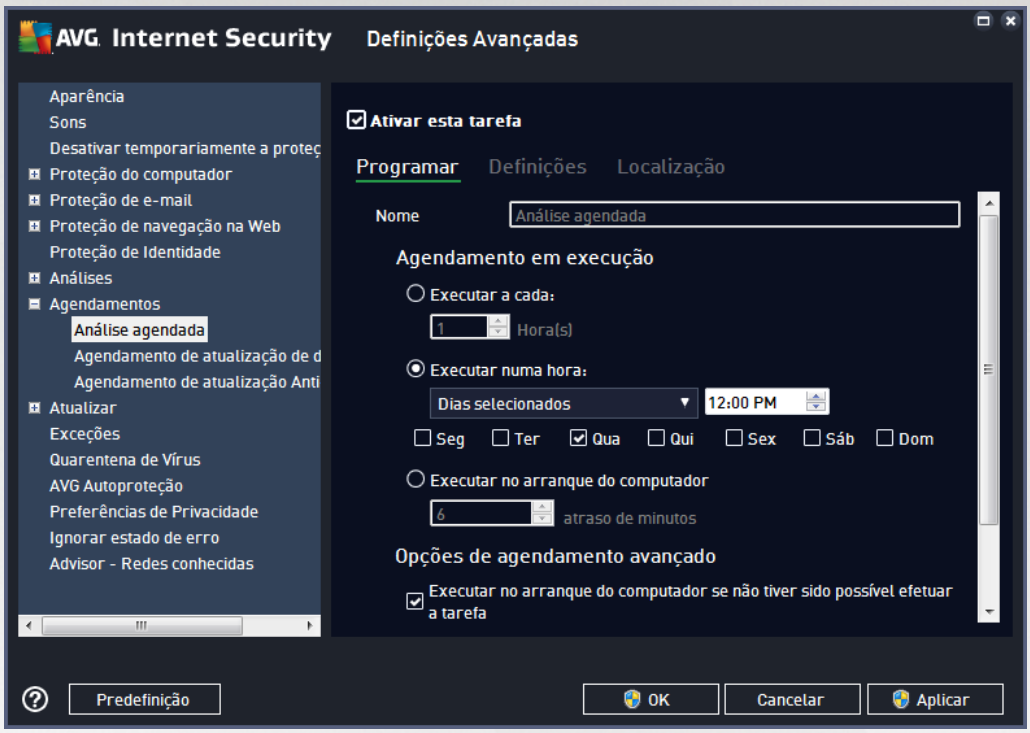
7.9. Agendamentos

Na secção ***Agendamentos*** pode editar as definições predefinidas do:

- Análise agendada
- Agendamento de atualização de definições
- Agendamento de atualização do programa
- Agendamento de atualização Anti-Spam

7.9.1. Análise agendada

Os parâmetros da análise agendada podem ser editados (*ou pode ser configurado um novo agendamento*) em três separadores. Em cada separador pode marcar/desmarcar o item ***Ativar esta tarefa*** para desativar temporariamente a análise agendada e voltar a ativá-la conforme necessário:



Em seguida, o campo de texto ***Nome*** (*desativado para todos os agendamentos predefinidos*) indica o nome atribuído ao agendamento atual pelo fornecedor do software. Para agendamentos novos (*pode adicionar um novo agendamento clicando com o botão direito do rato no item* ***Análise agendada*** *na árvore de navegação à esquerda*) pode especificar um nome da sua preferência e, nessas situações, o campo de texto será aberto para edição. Tente utilizar nomes curtos, descritivos e apropriados de análises para que futuramente seja mais fácil distinguir as análises de outras que venha a definir.

Exemplo: *não é adequado nomear uma análise com o nome "Nova análise" ou "A minha análise" uma vez que estes nomes não referem o que a análise efetivamente analisa. Por outro lado, um exemplo de um bom nome descritivo seria "Análise das áreas de sistema", etc. Também não é necessário especificar no nome da análise se a análise é de todo o computador ou somente de ficheiros e pastas selecionados – as suas próprias análises serão sempre uma versão específica da análise de ficheiros e pastas selecionados.*

Nesta janela pode ainda definir os seguintes parâmetros de análise:

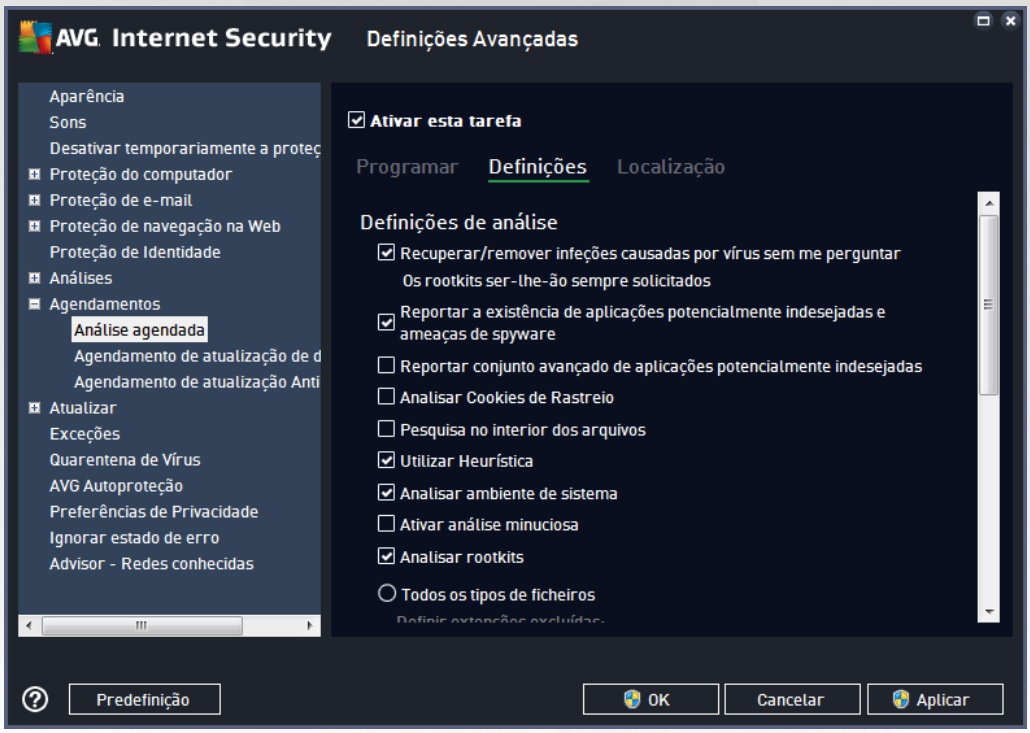
Agendamento em execução

Aqui, pode especificar os intervalos de tempo para a execução da nova análise agendada. A temporização pode ser definida pela execução repetida da análise após um determinado período de tempo (***Executar a cada...***) ou definindo uma data e hora exatas (***Executar a horas específicas***), ou ainda definindo um evento ao qual a execução da análise esteja associada (***Executar no arranque do computador***).

Opções de agendamento avançado

- ***Executar no arranque do computador se não tiver sido possível efetuar a tarefa*** – se agendar a tarefa para ser executada a uma hora específica, esta opção irá assegurar que a análise será executada posteriormente na eventualidade de o computador estar desligado à hora agendada.

- ***Executar mesmo se o computador estiver na opção de poupança de energia*** – a tarefa deve ser executada mesmo que o computador esteja a funcionar com bateria à hora agendada.



No separador ***Definições*** encontrará uma lista de parâmetros de análise que podem ser opcionalmente ativados/desativados. A maioria dos parâmetros estão ativados por predefinição e a funcionalidade será aplicada durante a análise. ***A menos que tenha uma razão válida para alterar estas definições, recomendamos que mantenha a configuração predefinida***:

- ***Recuperar/remover infeções causadas por vírus sem me perguntar*** *(ativado por predefinição):* se um vírus for detetado durante a análise, pode ser recuperado automaticamente se houver uma cura disponível. Se não for possível recuperar o ficheiro infetado automaticamente, o objeto infetado será movido para a Quarentena de Vírus.

- ***Reportar aplicações potencialmente indesejadas e ameaças de spyware*** *(ativado por predefinição):* marque esta opção para ativar a análise que procura spyware e também vírus. O Spyware representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade ativada, uma vez que aumenta a segurança do seu computador.

- ***Reportar conjunto avançado de aplicações potencialmente indesejadas*** (*desativado por*

predefinição): marque esta opção para detetar pacotes expandidos de spyware: programas que são perfeitamente fidedignos e inofensivos quando adquiridos diretamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, poderá bloquear programas legais e está, como tal, desativada por predefinição.

- ***Analisar Cookies de Rastreio*** (*desativado por predefinição*): este parâmetro especifica que os cookies deverão ser detetados durante a análise (*os cookies HTTP são utilizados para autenticação, rastreio e manutenção de informação específica dos utilizadores, tal como preferências de sites ou os conteúdos dos carrinhos de compras eletrónicos dos mesmos*).

- ***Pesquisa no interior dos arquivos*** (*desativado por predefinição*): este parâmetro especifica que a análise deverá verificar todos os ficheiros mesmo se estes estiverem comprimidos em arquivos, ex.: ZIP, RAR, etc.

- ***Utilizar Heurística*** (*ativado por predefinição*): a análise heurística (*emulação dinâmica das instruções do objeto analisado num ambiente de computador virtual*) será um dos métodos utilizados para a deteção de vírus durante a análise.

- ***Analisar ambiente de sistema*** (*ativado por predefinição*): a análise verificará também as áreas de sistema do seu computador.

- ***Ativar análise minuciosa*** (*desativado por predefinição):* em situações específicas (*suspeita de infeção do computador*) pode marcar esta opção para ativar os algoritmos de análise mais rigorosos que irão analisar todas as áreas do seu computador, incluindo as que raramente são infetadas, por precaução. Tenha em consideração que este método é bastante demorado.

- ***Analisar rootkits*** *(ativado por predefinição):* a análise Anti-Rootkit analisa o computador para procurar possíveis rootkits, ou seja, programas e tecnologias que podem ocultar atividade de malware no computador. Se for detetado um rootkit, isto não significa necessariamente que o computador esteja infetado. Em alguns casos, podem ser erroneamente detetados controladores específicos ou secções de aplicações seguras como sendo rootkits.

Também deve decidir se pretende analisar:

- ***Todos os tipos de ficheiros*** com a opção de definir exceções da análise ao indicar uma lista de extensões separadas por vírgula (*uma vez guardadas, as vírgulas mudam para ponto e vírgula*) que não devem ser analisadas.

- ***Tipos de ficheiros selecionados*** – pode especificar que pretende analisar apenas ficheiros que possam ser infetados (*ficheiros que não possam ser infetados não serão analisados, por exemplo, alguns ficheiros de texto simples ou outros ficheiros não executáveis*), incluindo ficheiros multimédia (*ficheiros de áudio, vídeo – se deixar esta caixa desmarcada, reduzirá o tempo de análise ainda mais, uma vez que os ficheiros são por vezes muito grandes e é pouco provável que estejam infetados por vírus*). Mais uma vez, pode especificar por extensões os ficheiros que deverão ser sempre analisados.

- Opcionalmente, pode decidir se pretende ***Analisar ficheiros sem extensão*** – esta opção está ativada por predefinição e é recomendável que a mantenha assim a menos que tenha uma razão válida para a alterar. Os ficheiros sem extensões são bastante suspeitos e devem ser sempre analisados.

Ajustar a rapidez de conclusão de uma Análise

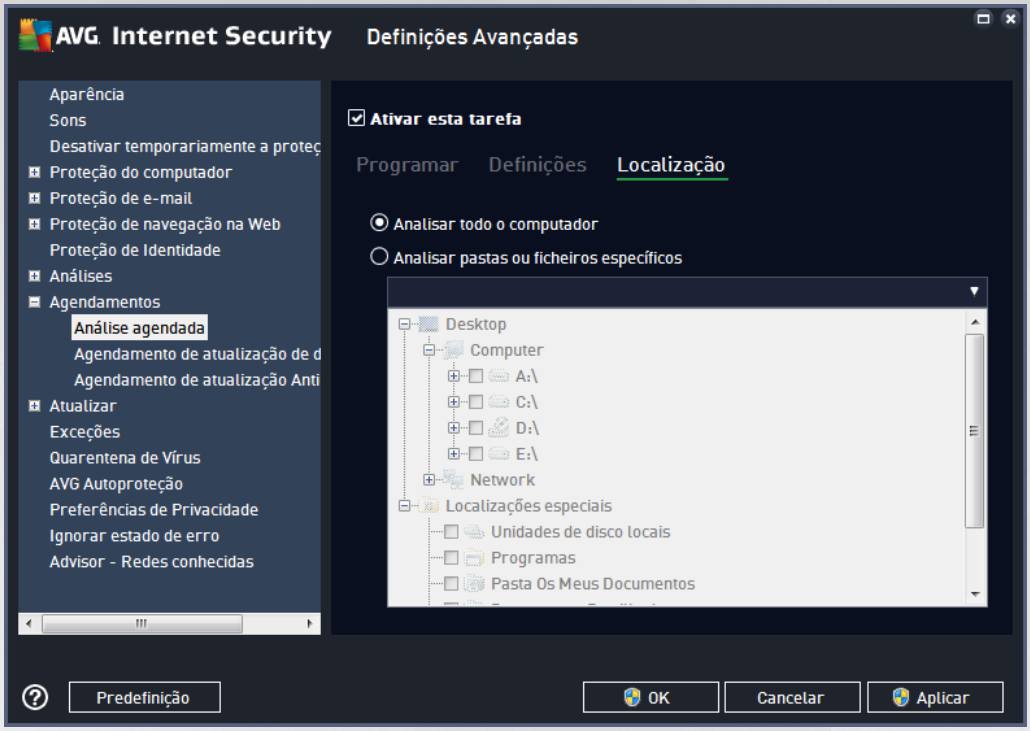
Nesta secção pode ainda especificar a velocidade de análise pretendida consoante a utilização dos recursos do sistema. Por predefinição, o valor desta opção está definido para o nível de *Opção do utilizador* de utilização automática de recursos. Se quiser que a análise seja executada mais rapidamente, esta demorará menos tempo, mas os recursos do sistema utilizados aumentarão significativamente durante a execução da análise e tal diminuirá o desempenho de outras atividades no PC (*esta opção pode ser utilizada quando o seu computador estiver ligado e ninguém o estiver a utilizar*). Por outro lado, pode diminuir os recursos do sistema utilizados prolongando a duração da análise.

Definir relatórios de análise adicionais

Clique na ligação ***Definir relatórios de análise adicionais...*** para abrir uma janela independente intitulada ***Relatórios de análise***, na qual pode selecionar vários itens para definir quais as deteções que deverão ser reportadas:

Opções de encerramento do computador

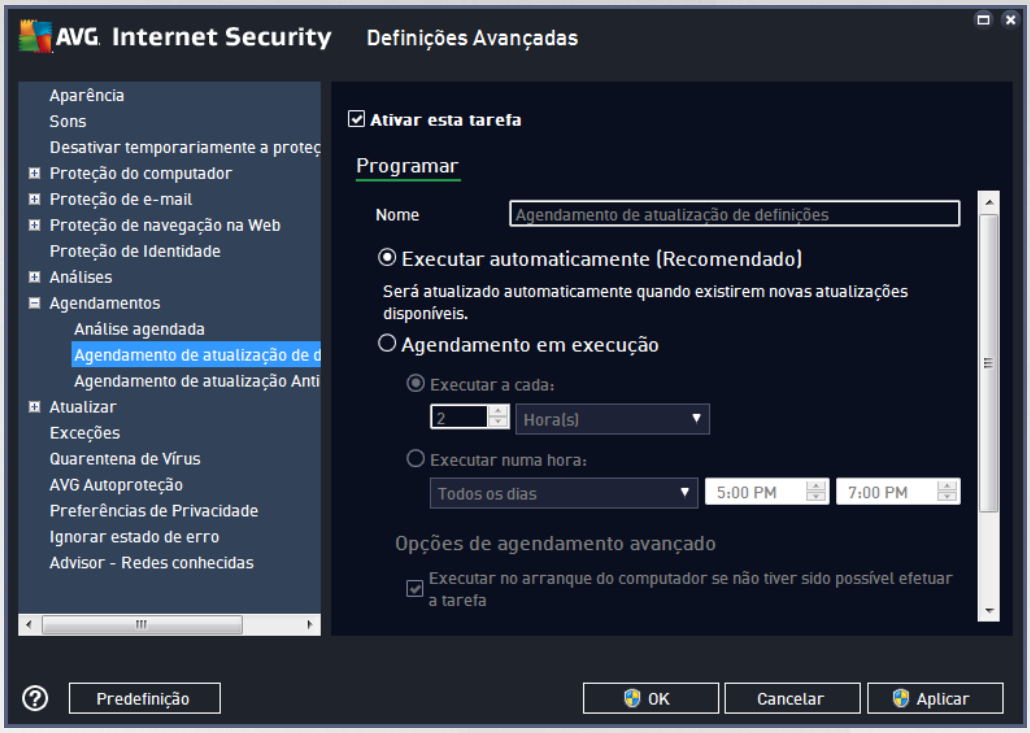
Na secção ***Opções de encerramento do computador*** pode decidir se o computador deve ser encerrado automaticamente uma vez concluído o processo de análise em execução. Tendo confirmado esta opção (***Encerrar o computador aquando da conclusão da análise***), será ativada uma nova opção que permite que o computador encerre mesmo que esteja bloqueado (***Forçar o encerramento se o computador estiver bloqueado***).



No separador ***Localização*** pode definir se pretende agendar uma análise de todo o computador ou uma análise de ficheiros ou pastas. Na eventualidade de selecionar a análise de ficheiros ou pastas, a estrutura em árvore apresentada na parte inferior desta janela é ativada e pode especificar as pastas a serem analisadas.

7.9.2. Agendamento de atualização de definições

Se for ***realmente necessário***, pode desmarcar o item ***Ativar esta tarefa*** para desativar temporariamente a atualização de definições e ativá-lo novamente mais tarde:



Nesta janela pode configurar alguns parâmetros detalhados do agendamento de atualização de definições. O campo de texto ***Nome*** (*desativado para todos os agendamentos predefinidos*) mostra o nome atribuído ao agendamento atual pelo fornecedor do software.

Agendamento em execução

Por predefinição, a tarefa é iniciada automaticamente (***Executar automaticamente***) assim que estiver disponível uma nova atualização de definições de vírus. É aconselhável manter esta configuração, a não ser que tenha uma boa razão para não o fazer! Em seguida, pode configurar o início da tarefa manualmente e especificar os intervalos de tempo para a execução da atualização de definições que foi agendada. A temporização pode ser definida pela execução repetida da atualização após um determinado período de tempo (***Executar a cada...***) ou definindo uma data e hora exatas (***Executar a horas específicas***).

Opções de agendamento avançado

Esta secção permite-lhe definir em que condições a atualização de definições deverá/não deverá ser executada se o computador estiver em modo de baixo consumo ou desligado.

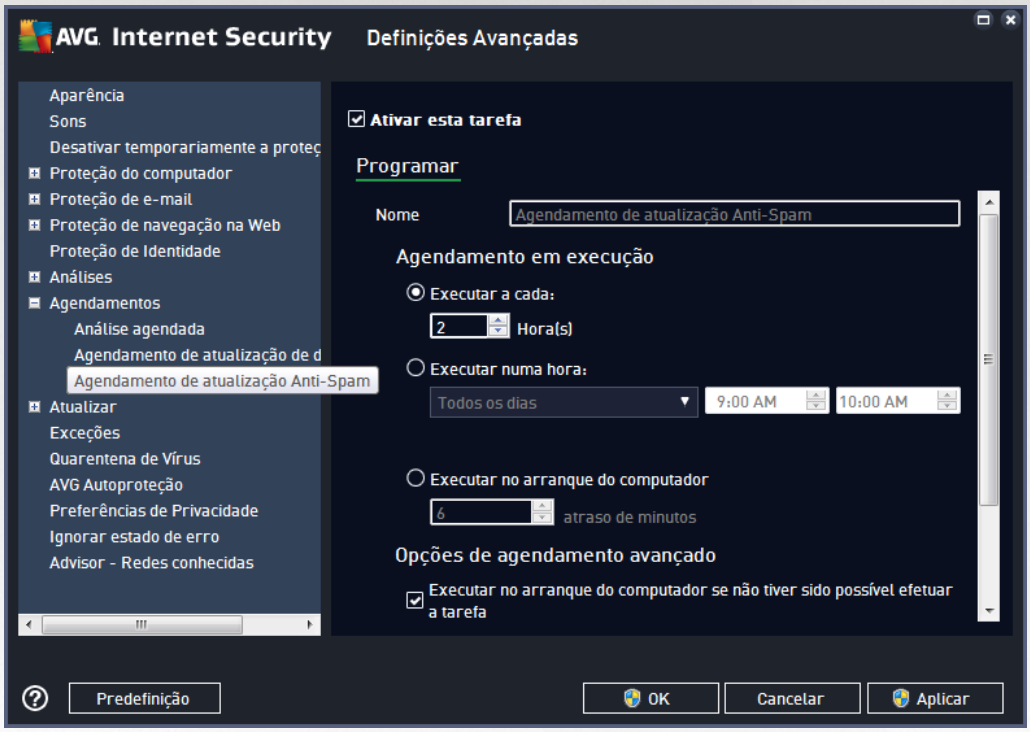
Outras definições de atualização

Por último, marque a opção ***Executar a atualização novamente quando a ligação de Internet estiver***

disponível para se certificar de que, se a ligação à Internet for interrompida e o processo de atualização falhar, a atualização será executada de novo imediatamente após o restabelecimento da ligação à Internet. Uma vez iniciada a atualização agendada à hora especificada, será informado desse facto através de uma janela pop-up aberta por cima do ícone do AVG na barra de tarefas (*desde que tenha mantido a configuração predefinida da janela Definições Avançadas/Aparência*).

7.9.3. Agendamento de atualização do programa

Se for ***efetivamente necessário***, pode desmarcar o item ***Ativar esta tarefa*** para desativar temporariamente a atualização do programa agendada e voltar a ativá-la posteriormente:



O campo de texto ***Nome*** (*desativado para todos os agendamentos predefinidos*) mostra o nome atribuído ao agendamento atual pelo fornecedor do software.

Agendamento em execução

Aqui, especifique os intervalos de tempo para a execução do novo agendamento de atualização do programa. A temporização pode ser definida pela execução repetida da atualização após um determinado período de tempo (***Executar a cada***) ou definindo uma data e hora exatas (***Executar a horas específicas***), ou ainda definindo um evento ao qual a execução da atualização esteja associada (***Executar no arranque do computador***).

Opções de agendamento avançado

Esta secção permite-lhe definir em que condições a atualização do programa deverá/não deverá ser executada se o computador estiver em modo de baixo consumo ou desligado.

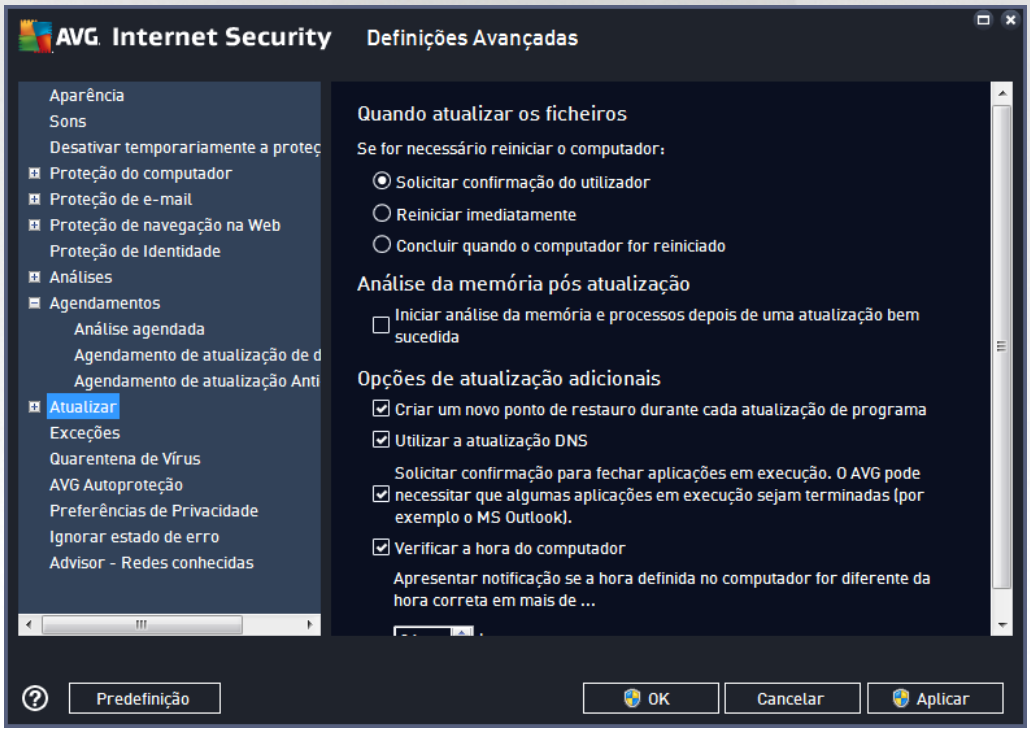
Outras definições de atualização

Marque a opção ***Executar a atualização novamente quando a ligação de Internet estiver disponível*** para se certificar de que, se a ligação à Internet for interrompida e o processo de atualização falhar, a atualização será executada de novo imediatamente após o restabelecimento da ligação à Internet. Uma vez iniciada a atualização agendada à hora especificada, será informado desse facto através de uma janela pop-up aberta por cima do ícone do AVG na barra de tarefas (*desde que tenha mantido a configuração predefinida da janela Definições Avançadas/Aparência*).

Nota: *se um agendamento de atualização do programa coincidir com uma análise agendada, o processo de atualização terá precedência e a análise será interrompida. Nesse caso, será informado do conflito.*

7.9.4. Agendamento de atualização Anti-Spam

Se for necessário, pode desmarcar o item ***Ativar esta tarefa***, simplesmente para desativar a atualização agendada do Anti-Spam temporariamente e ativá-la novamente mais tarde:


AVG Internet Security
Definições Avançadas
Aparência
Sons
Desativar temporariamente a proteç
Proteção do computador
Proteção de e-mail
Proteção de navegação na Web
Proteção de Identidade
Análises
Agendamentos
Análise agendada
Agendamento de atualização de d
Agendamento de atualização Anti
Atualizar
Exceções
Quarentena de Vírus
AVG Autoproteção
Preferências de Privacidade
Ignorar estado de erro
Advisor - Redes conhecidas
Quando atualizar os ficheiros
Se for necessário reiniciar o computador:
Solicitar confirmação do utilizador
Reiniciar imediatamente
Concluir quando o computador for reiniciado
Análise da memória pós atualização
Iniciar análise da memória e processos depois de uma atualização bem sucedida
Opções de atualização adicionais
Criar um novo ponto de restauro durante cada atualização de programa
Utilizar a atualização DNS
Solicitar confirmação para fechar aplicações em execução. O AVG pode necessitar que algumas aplicações em execução sejam terminadas (por exemplo o MS Outlook).
Verificar a hora do computador
Apresentar notificação se a hora definida no computador for diferente da hora correta em mais de ...
Predefinição
OK
Cancelar
Aplicar

Nesta janela pode configurar alguns parâmetros detalhados do agendamento de atualização. O campo de texto ***Nome*** (*desativado para todos os agendamentos predefinidos*) indica o nome atribuído ao agendamento atual pelo fornecedor do software.

Agendamento em execução

Aqui, especifique os intervalos de tempo para a execução de novos agendamentos de atualização do Anti-Spam. A temporização pode ser definida pela execução repetida da atualização do Anti-Spam após um determinado período de tempo (***Executar a cada***) ou definindo uma data e hora exatas (***Executar a horas específicas***), ou ainda definindo um evento ao qual a execução da atualização esteja associada (***Executar no***

arranque do computador).

Opções de agendamento avançado

Esta secção permite-lhe definir em que condições a atualização do Anti-Spam deverá/não deverá ser executada se o computador estiver em modo de baixo consumo ou desligado.

Outras definições de atualização

Marque a opção ***Executar a atualização novamente quando a ligação de Internet estiver disponível*** para se certificar de que, se a ligação à Internet for interrompida e o processo de atualização do componente Anti-Spam falhar, a atualização será executada de novo imediatamente após o restabelecimento da ligação à Internet. Uma vez iniciada a análise agendada à hora especificada, será informado desse facto através de uma janela pop-up aberta por cima do ícone do AVG na barra de tarefas (*desde que tenha mantido a configuração predefinida da janela Definições Avançadas/Aparência*).

7.10. Atualizar

O item de navegação ***Atualizar*** abre uma nova janela onde pode especificar parâmetros gerais relativos à atualização do AVG:

AVG Internet Security
Definições Avançadas
Aparência
Sons
Desativar temporariamente a proteç
Proteção do computador
Proteção de e-mail
Proteção de navegação na Web
Proteção de Identidade
Análises
Agendamentos
Atualizar
Proxy
Gerir
Exceções
Quarentena de Vírus
AVG Autoproteção
Preferências de Privacidade
Ignorar estado de erro
Advisor - Redes conhecidas
Quando atualizar os ficheiros
Se for necessário reiniciar o computador:
Solicitar confirmação do utilizador
Reiniciar imediatamente
Concluir quando o computador for reiniciado
Análise da memória pós atualização
Iniciar análise da memória e processos depois de uma atualização bem sucedida
Opções de atualização adicionais
Criar um novo ponto de restauro durante cada atualização de programa
Utilizar a atualização DNS
Solicitar confirmação para fechar aplicações em execução. O AVG pode necessitar que algumas aplicações em execução sejam terminadas (por exemplo o MS Outlook).
Verificar a hora do computador
Apresentar notificação se a hora definida no computador for diferente da hora correta em mais de ...
Predefinição
OK
Cancelar
Aplicar

Quando atualizar os ficheiros

Nesta secção pode optar entre três alternativas a serem usadas caso o processo de atualização requeira a reinicialização do PC. A conclusão do processo de atualização pode ser agendada para o próximo arranque

do PC ou pode executar a reinicialização imediatamente:

- ***Solicitar confirmação do utilizador*** *(ativado por predefinição)* – ser-lhe-á pedido que aprove um reinício do PC necessário para finalizar o processo de atualização
- ***Reiniciar imediatamente*** – o computador será reiniciado automaticamente depois de o processo de atualização terminar e a sua aprovação não será necessária
- ***Concluir quando o computador for reiniciado*** – a conclusão do processo de atualização será adiada até ao próximo arranque do computador. Tenha em conta que esta opção só é recomendada se tiver a certeza de que o computador é ligado e desligado com regularidade, pelo menos uma vez por dia!

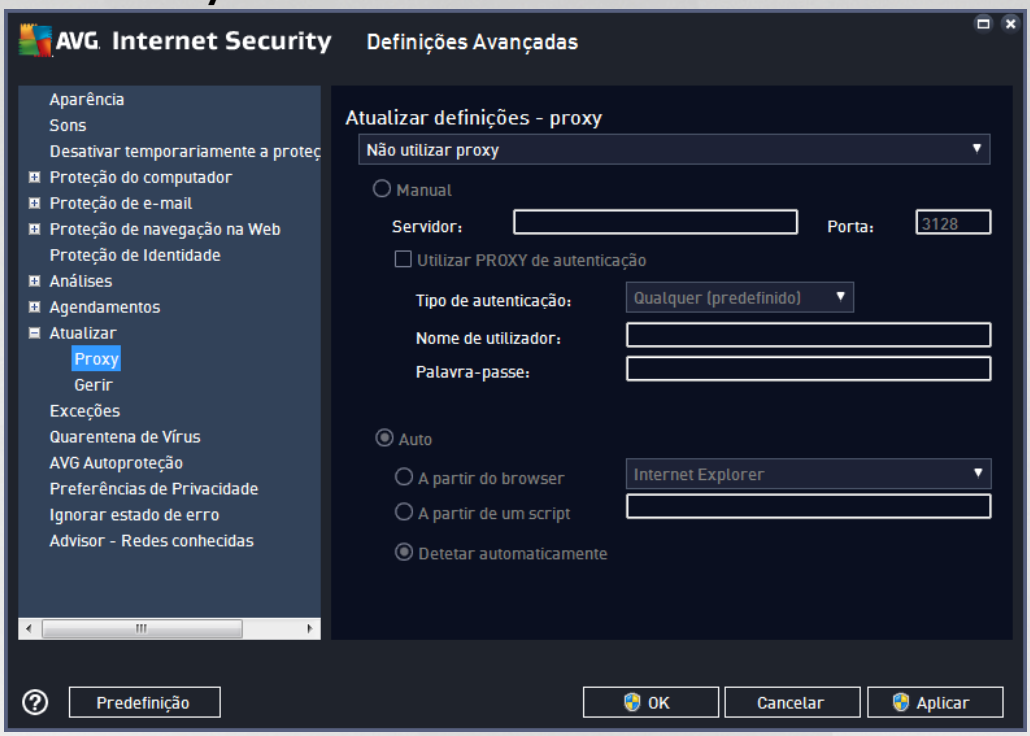
Análise da memória pós atualização

Marque esta caixa para indicar que pretende iniciar uma nova análise da memória após cada atualização bem sucedida. A atualização transferida pode ter novas definições de vírus e estas podem ser aplicadas na análise imediatamente.

Opções de atualização adicionais

- ***Criar um novo ponto de restauro durante cada atualização de programa*** (*ativado por predefinição*) – antes da execução de cada atualização de programa do AVG, é criado um ponto de restauro do sistema. Na eventualidade de o processo de atualização falhar e o seu sistema operativo falhar, pode sempre restaurar o seu SO para a configuração original a partir deste ponto. Pode aceder a esta opção através de Iniciar / Todos os Programas / Acessórios / Ferramentas do Sistema / Restauro do Sistema, mas quaisquer alterações são recomendadas apenas a utilizadores avançados! Mantenha esta caixa selecionada se quiser utilizar esta funcionalidade.
- ***Utilizar a atualização DNS*** (*ativado por predefinição*) – com este item marcado, uma vez iniciada a atualização, o **AVG Internet Security** procura informações relativas à última versão da base de dados de vírus e à mais recente versão do programa no servidor DNS. Então, só são transferidos e aplicados os ficheiros de atualização mais pequenos e indispensáveis. Desta forma, a quantidade total de dados transferidos é minimizada e o processo de atualização é executado mais depressa.
- ***Solicitar confirmação para fechar aplicações em execução*** (*ativado por predefinição*) – ajuda a assegurar que não serão fechadas quaisquer aplicações em execução sem a sua permissão (se necessário para que o processo de atualização seja concluído).
- ***Verificar a hora do computador*** (*ativado por predefinição*) – marque esta opção para indicar que pretende que sejam apresentadas notificações na eventualidade de a hora do computador ser diferente da hora correta além do número de horas especificado.

7.10.1. Proxy



O servidor proxy é um servidor autónomo ou um serviço executado no computador que garante uma ligação mais segura à Internet. De acordo com as regras de rede especificadas, pode aceder à Internet diretamente ou através do servidor proxy; as duas possibilidades podem ser permitidas em simultâneo. Depois, no primeiro item da janela ***Definições de atualização – proxy*** pode selecionar a partir do menu da janela de sequência se pretender:

- ***Não utilizar proxy*** – predefinições
- ***Utilizar proxy***
- ***Tentar ligação utilizando proxy e se falhar, ligar diretamente***

Se selecionar qualquer opção utilizando o servidor proxy, terá de especificar mais alguns dados. As definições do servidor podem ser configuradas manualmente ou automaticamente.

Configuração manual

Se selecionar a configuração manual (marque *a opção* ***Manual*** *para ativar a secção respetiva da janela*), tem de especificar os seguintes itens:

- ***Servidor*** – especifique o endereço IP do servidor ou o nome do servidor
- ***Porta*** – especifique o número da porta que permite aceder à Internet (*por predefinição, este número está configurado para 3128, mas pode ser configurado para um número diferente – se não tiver a certeza, contacte o administrador da rede*)

O servidor proxy também pode ter regras específicas configuradas para cada utilizador. Se o seu servidor proxy estiver configurado desta forma, selecione a opção ***Utilizar PROXY de autenticação*** para verificar se o seu nome de utilizador e palavra-passe são válidos para estabelecer ligação à Internet através do servidor proxy.

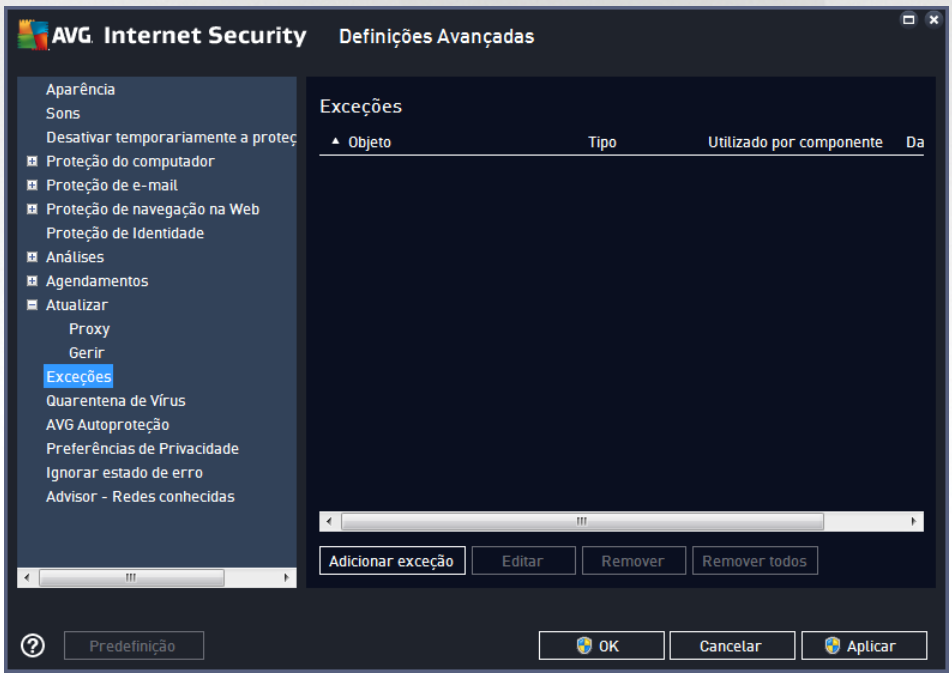
Configuração automática

Se selecionar a configuração automática (*marque a opção **Auto** para ativar a secção respetiva da janela*), selecione depois de onde a configuração proxy deve ser retirada:

- ***A partir do browser*** – a configuração será lida a partir do seu browser predefinido
- ***A partir de um script*** – a configuração será lida a partir do script transferido com a função a devolver o endereço do proxy
- ***Detetar automaticamente*** – a configuração será detetada automática e diretamente a partir do servidor proxy

7.10.2. Gerir

A janela ***Gestão de atualizações*** disponibiliza duas opções acessíveis através de dois botões:

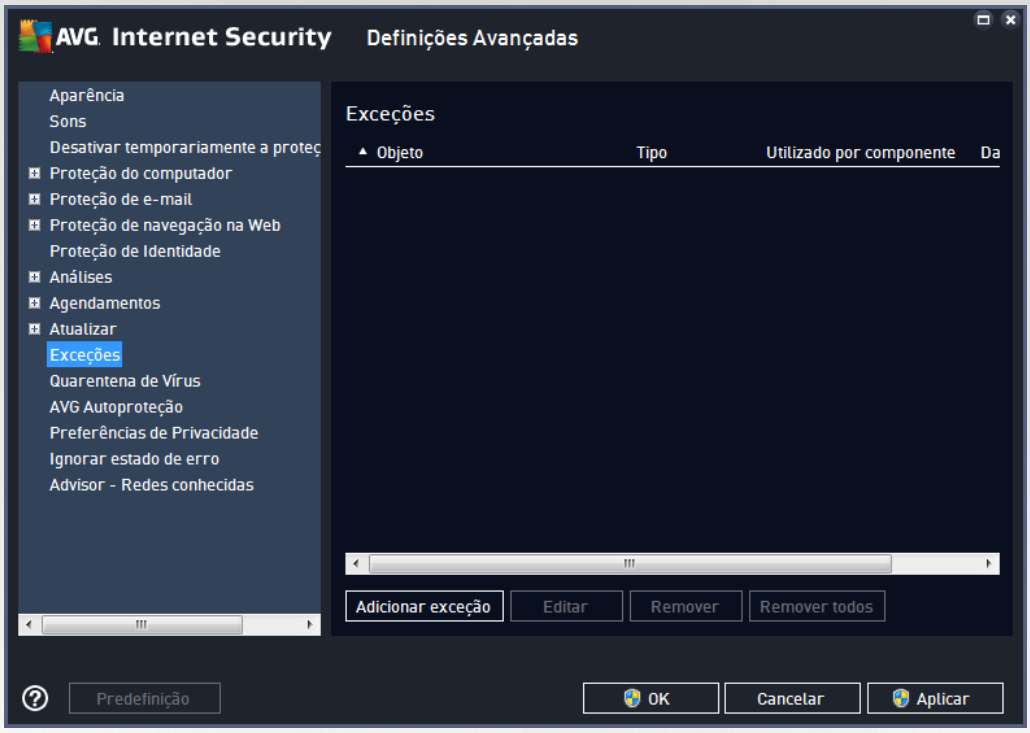


- ***Eliminar os ficheiros de atualização temporários*** – clique neste botão para eliminar todos os ficheiros de atualização desnecessários do seu disco rígido (*por predefinição, estes ficheiros são guardados durante 30 dias*)
- ***Reverter a base de dados de vírus para a versão anterior*** – clique neste botão para eliminar a última versão da base de dados de vírus do seu disco rígido e para regressar à versão anteriormente guardada (*a nova versão de base de dados de vírus fará parte da atualização seguinte*)

7.11. Exceções

Na janela ***Exceções*** pode definir exceções, ou seja, itens que devem ser ignorados pelo **AVG Internet Security**. Normalmente, será necessário definir uma exceção se o AVG continuar a detetar um programa ou ficheiro como uma ameaça, ou a bloquear um site seguro como sendo perigoso. Adicione esse ficheiro ou site à lista de exceções e o AVG deixará de reportá-lo ou bloqueá-lo.

Certifique-se sempre de que o ficheiro, programa ou site em questão é de facto totalmente seguro!



A tabela que aparece na janela apresenta uma lista de exceções, se já tiverem sido definidas exceções. Existe uma caixa de verificação junto de cada item. Se a caixa estiver assinalada, a exceção está ativada; caso contrário, a exceção está definida, mas não está ativada. Ao clicar no cabeçalho de uma coluna, pode ordenar os itens permitidos de acordo com os critérios respetivos.

Botões de controlo

- ***Adicionar exceção*** – Clique para abrir uma nova janela, na qual poderá especificar o item que deve ser excluído da análise do AVG.

AVG Internet Security
Tipo de exceção:
Aplicação ou ficheiro
Escolha o ficheiro que NÃO quer que seja analisado
Procurar
Ignorar este ficheiro:
Mesmo se o ficheiro for movido para uma nova localização
Mesmo se o ficheiro tiver sido alterado ou atualizado
Utilize esta exceção para:
Proteção Residente (se estiver marcado, o AVG NÃO analisará o ficheiro ou a aplicação quando forem abertos)
Análise agendada e manual (se estiver marcado, o AVG NÃO analisará este ficheiro durante análises)
Proteção de Identidade (se estiver marcado, o AVG NÃO monitorizará a aplicação para detetar comportamento malicioso)
Proteção Online (se estiver marcado, o AVG NÃO analisará as atividades online da aplicação)
OK
Cancelar

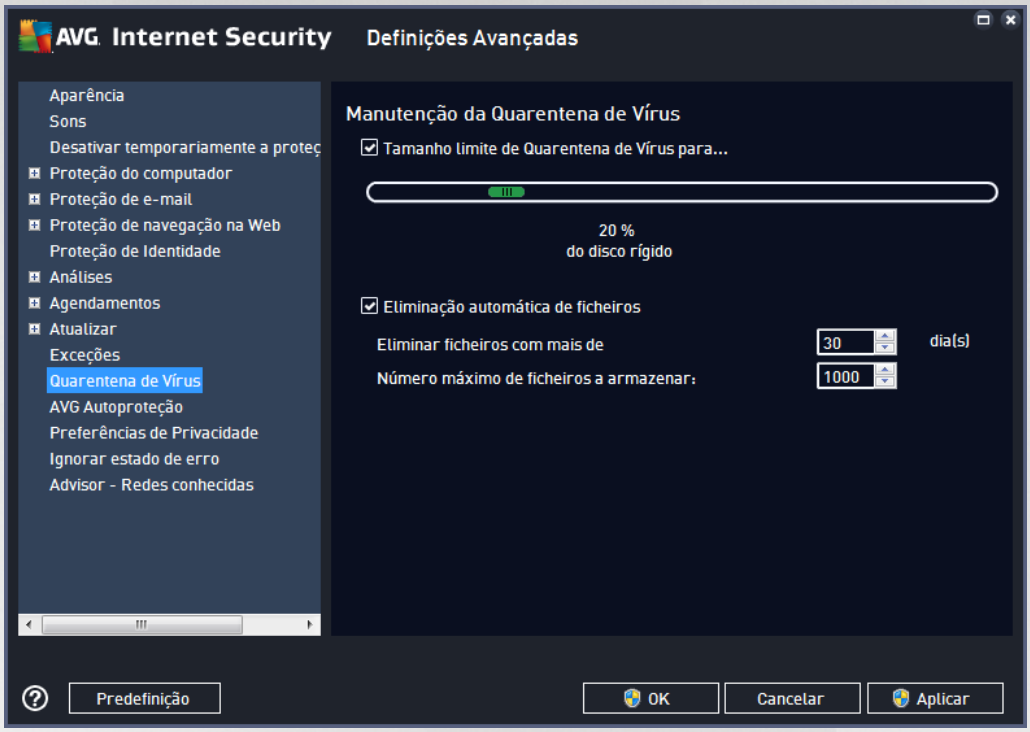
Em primeiro lugar, ser-lhe-á pedido que defina o tipo de objeto, ou seja, se é uma aplicação ou um ficheiro, uma pasta, um URL ou um certificado. Em seguida, terá de procurar no disco a localização do objeto em questão ou digitar o URL. Por último, pode selecionar as funcionalidades do AVG que devem ignorar o objeto selecionado *(Proteção Residente, Proteção de Identidade, Analisar)*.

- ***Editar*** – Este botão só fica ativo se já tiverem sido definidas algumas exceções e se estas estiverem incluídas na tabela. Em seguida, pode utilizar o botão para abrir a janela de edição sobre uma exceção selecionada e configurar os parâmetros da exceção.

- ***Remover*** – Utilize este botão para cancelar uma exceção definida anteriormente. Pode remover as exceções individualmente ou realçar um conjunto de exceções na lista e cancelar as exceções definidas. Depois de cancelar a exceção, o ficheiro, a pasta ou o URL em questão será novamente analisado pelo AVG. Tenha em atenção que apenas a exceção será removida, não o ficheiro ou a pasta em si!

- ***Remover tudo*** – Utilize este botão para eliminar todas as exceções definidas na lista.

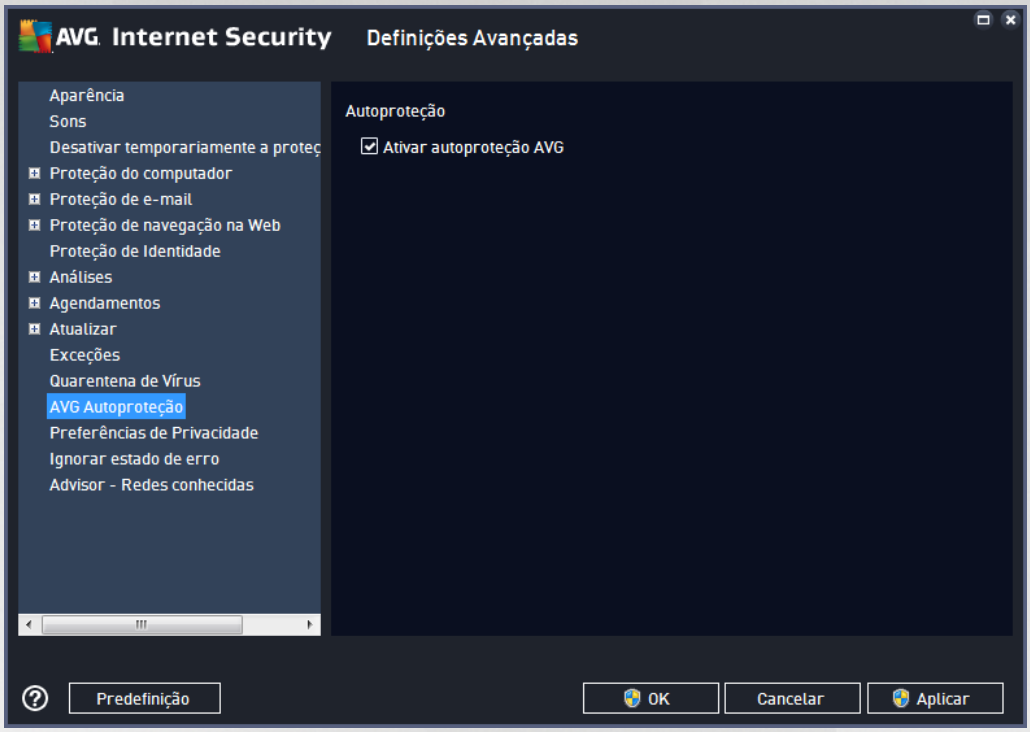
7.12. Quarentena de Vírus



A janela ***Manutenção da Quarentena de Vírus*** permite definir vários parâmetros relacionados com a administração dos objetos armazenados na Quarentena de Vírus:

- ***Tamanho limite de Quarentena de Vírus*** – utilize o cursor para definir o tamanho máximo da Quarentena de Vírus. O tamanho é especificado proporcionalmente ao tamanho do seu disco local.
- ***Eliminação automática de ficheiros*** – nesta secção defina o tempo máximo que os objetos deverão ficar armazenados na Quarentena de Vírus (***Eliminar ficheiros com mais de ... dias***) e o número máximo de ficheiros a armazenar na Quarentena de Vírus (***Número máximo de ficheiros a armazenar***).

7.13. AVG Autoproteção

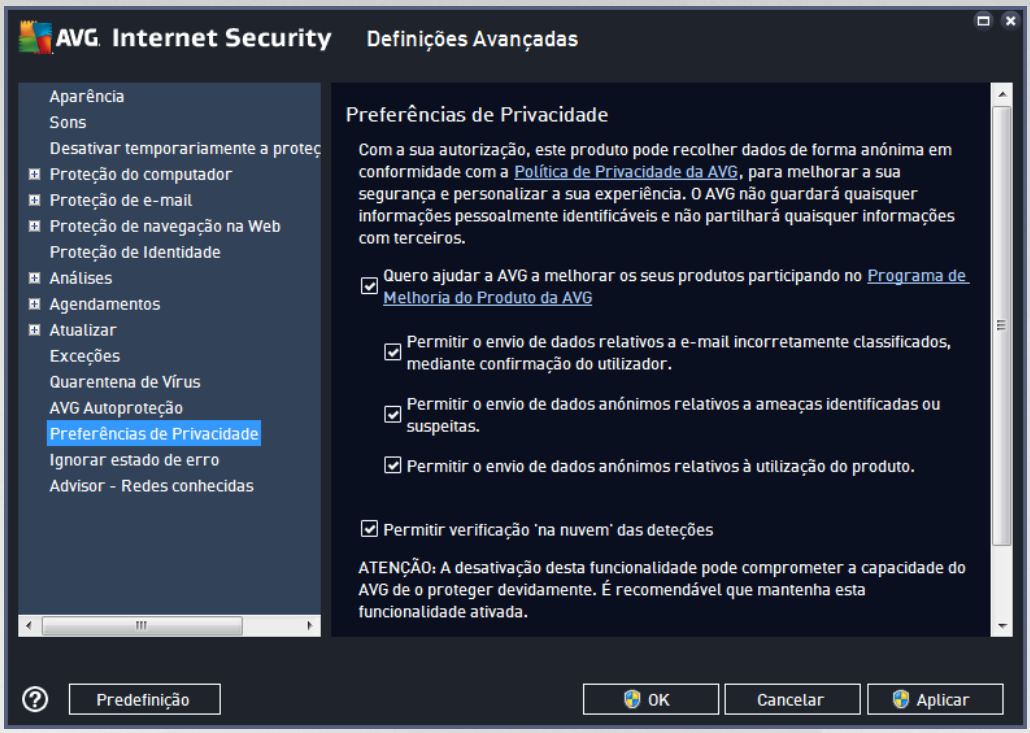


A funcionalidade ***AVG Autoproteção*** permite ao **AVG Internet Security** proteger os seus próprios processos, ficheiros, chaves de registo e controladores contra alteração ou desativação. Este tipo de proteção tem como finalidade principal evitar que determinadas ameaças sofisticadas tentem desativar a proteção antivírus e causar danos livremente no computador.

É aconselhável manter esta funcionalidade ativada!

7.14. Preferências de Privacidade

A janela ***Preferências de Privacidade*** convida-o a participar na melhoria do produto AVG e a ajudar-nos a aumentar o nível de segurança da Internet em geral. A comunicação ajuda-nos a recolher informação atualizada relativa às mais recentes ameaças de participantes de todo o mundo, e em troca podemos melhorar a proteção para todos. A comunicação é feita automaticamente, sem causar qualquer incómodo ao utilizador. Não são incluídos dados pessoais nos relatórios. A comunicação de ameaças detetadas é opcional; contudo, pedimos que mantenha esta opção ativada. Ajuda-nos a melhorar a proteção para o utilizador em particular e todos os utilizadores do AVG em geral.


AVG Internet Security
Definições Avançadas
Aparência
Sons
Desativar temporariamente a proteç
Proteção do computador
Proteção de e-mail
Proteção de navegação na Web
Proteção de Identidade
Análises
Agendamentos
Atualizar
Exceções
Quarentena de Vírus
AVG Autoproteção
Preferências de Privacidade
Ignorar estado de erro
Advisor - Redes conhecidas
Preferências de Privacidade
Com a sua autorização, este produto pode recolher dados de forma anónima em conformidade com a Política de Privacidade da AVG, para melhorar a sua segurança e personalizar a sua experiência. O AVG não guardará quaisquer informações pessoalmente identificáveis e não partilhará quaisquer informações com terceiros.
Quero ajudar a AVG a melhorar os seus produtos participando no Programa de Melhoria do Produto da AVG
Permitir o envio de dados relativos a e-mail incorretamente classificados, mediante confirmação do utilizador.
Permitir o envio de dados anónimos relativos a ameaças identificadas ou suspeitas.
Permitir o envio de dados anónimos relativos à utilização do produto.
Permitir verificação 'na nuvem' das deteções
ATENÇÃO: A desativação desta funcionalidade pode comprometer a capacidade do AVG de o proteger devidamente. É recomendável que mantenha esta funcionalidade ativada.
Predefinição
OK
Cancelar
Aplicar

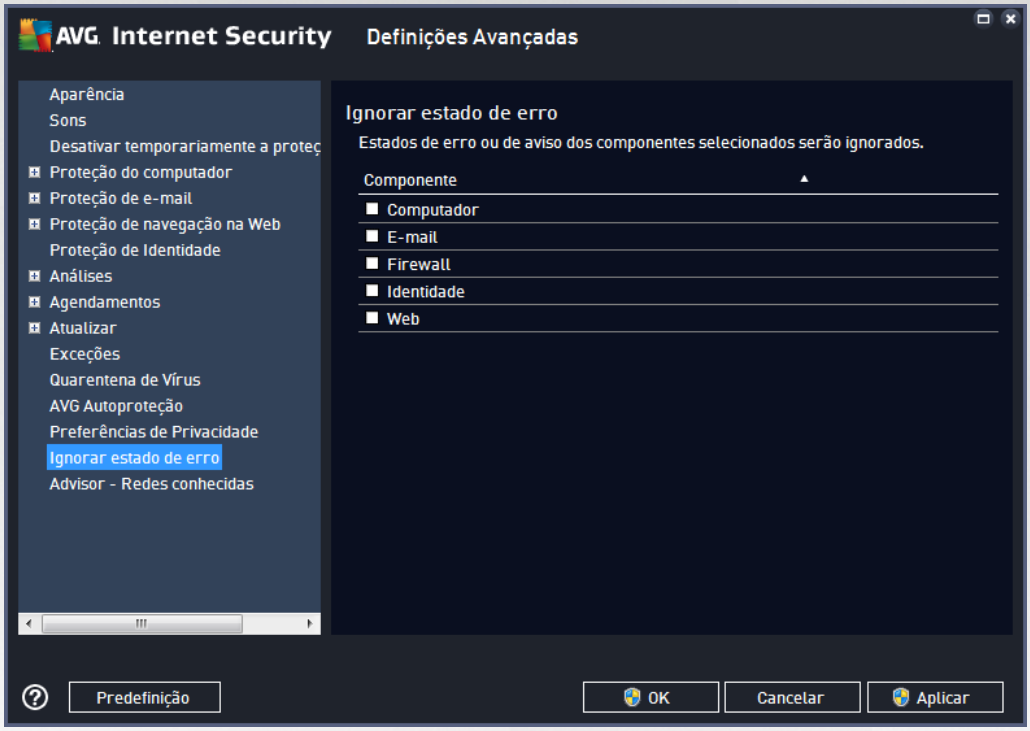
Nesta janela, estão disponíveis as seguintes opções de configuração:

- ***Quero ajudar a AVG a melhorar os seus produtos participando no Programa de Melhoria do Produto da AVG*** *(ativado por predefinição)* – Se quiser ajudar-nos a melhorar ainda mais o **AVG Internet Security**, mantenha a caixa assinalada. Isso permite que todas as ameaças detetadas sejam comunicadas à AVG, para que possamos recolher informações atualizadas sobre malware de todos os participantes a nível mundial e, como compensação, melhorar a proteção para todos. A comunicação é feita automaticamente, como tal não lhe causa qualquer inconveniente, e não são incluídos nos relatórios quaisquer dados pessoais.
    - ***Permitir o envio de dados relativos a e-mails incorretamente classificados, mediante confirmação do utilizador*** *(ativado por predefinição)* – enviar informações sobre mensagens de e-mail incorretamente identificadas como spam ou sobre mensagens de spam que não foram detetadas pelo serviço Anti-Spam. Ao enviar este tipo de informações, ser-lhe-á pedida confirmação.
    - ***Permitir o envio de dados anónimos relativos a ameaças identificadas ou suspeitas*** *(ativado por predefinição)* – enviar informações sobre qualquer código ou padrão de comportamento suspeito ou identificado como perigoso *(pode ser um vírus, spyware ou uma página Web maliciosa a que esteja a tentar aceder)* detetado no seu computador.
    - ***Permitir o envio de dados anónimos relativos à utilização do produto*** *(ativado por predefinição)* – enviar estatísticas básicas sobre a utilização da aplicação, tais como o número de deteções, análises executadas, atualizações bem/mal sucedidas, etc.
- ***Permitir verificação 'na nuvem' das deteções*** *(ativado por predefinição)* – as ameaças detetadas serão verificadas em termos efetivos de infeção, para identificar falsos positivos.
- ***Quero que o AVG personalize a minha experiência ativando a Personalização do AVG***

(desativado por predefinição) – esta funcionalidade analisa de forma anónima o comportamento de programas e aplicações instalados no computador. Com base nessa análise, o AVG pode disponibilizar serviços adequados às suas necessidades para assegurar segurança máxima.

7.15. Ignorar estado de erro

Na janela ***Ignorar estado de erro*** pode selecionar os componentes sobre os quais não quer ser informado:



Por predefinição, nenhum dos componentes na lista está selecionado. Isso significa que se algum componente obtiver um estado de erro, será informado imediatamente dessa situação através de:

- ícone da barra de tarefas – enquanto todos os componentes do AVG estiverem a funcionar devidamente, o ícone é apresentado com quatro cores; no entanto, se ocorrer um erro, os ícones serão apresentados com um ponto de exclamação amarelo
- uma descrição textual do problema existente na secção Informação de Estado de Segurança da janela principal do AVG

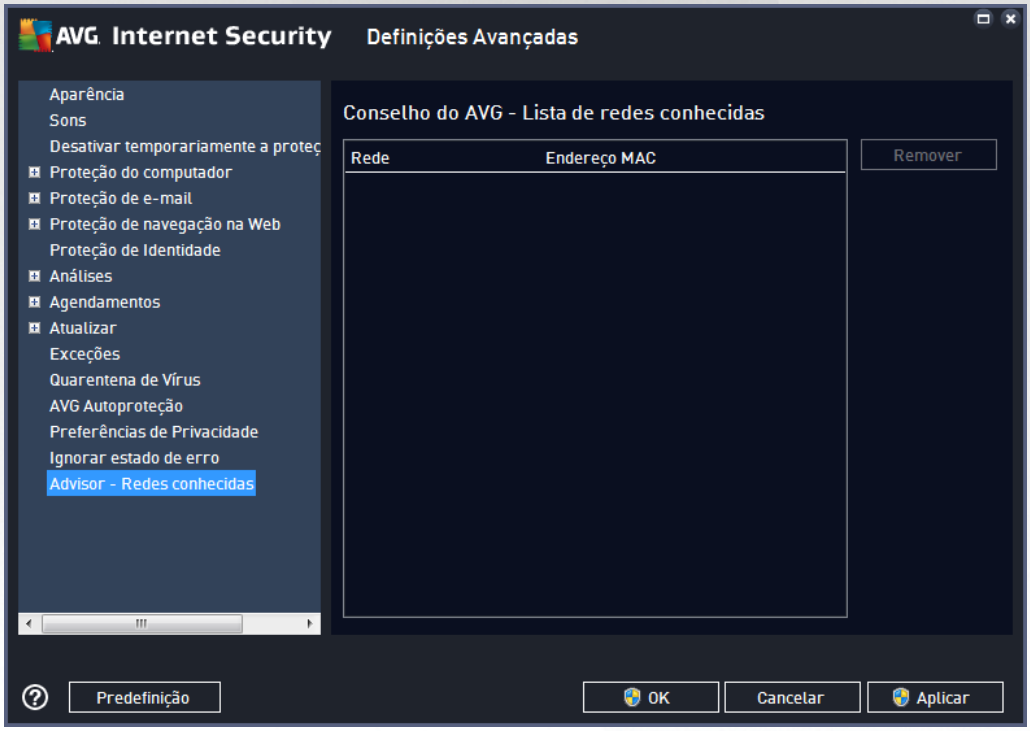
Poderá verificar-se uma situação em que, por qualquer motivo, será necessário desativar um componente temporariamente. ***Essa ação não é recomendada, deve procurar manter todos os componentes ativados permanentemente e com a configuração predefinida***, mas poderá acontecer. Nesse caso, o ícone da barra de tarefas reporta automaticamente o estado de erro do componente. No entanto, nesta situação não podemos considerar um erro efetivo uma vez que o utilizador ocasionou-o deliberadamente e tem consciência do risco potencial. Em simultâneo, uma vez apresentado a cinzento, o ícone não poderá apresentar quaisquer outros erros que possam surgir.

Nesta eventualidade, pode selecionar componentes na janela ***Ignorar estado de erro*** que possam estar em estado de erro (*ou desativados*) e estabelecer que não pretende ser informado dos mesmos. Clique no botão ***OK*** para confirmar.

7.16. Advisor – Redes conhecidas

O Conselho do AVG inclui uma funcionalidade que monitoriza as redes às quais o utilizador estabelece ligação e, se for encontrada uma nova rede *(com um nome de rede que já é utilizado, o que pode ser confuso)*, avisa o utilizador e recomenda a verificação da segurança da rede. Se decidir que é seguro estabelecer ligação à nova rede, também pode guardar a rede nesta lista *(através da ligação disponibilizada na notificação do Conselho do AVG que aparece por cima da barra de tarefas quando é detetada uma rede desconhecida. Para mais informações, consulte o capítulo referente ao Conselho do AVG)*. O Conselho do AVG memorizará os atributos exclusivos da rede *(especificamente o endereço MAC)* e não voltará a apresentar a notificação. Cada rede à qual o utilizador estabelecer ligação será considerada automaticamente uma rede conhecida e será adicionada à lista. Pode eliminar entradas individuais clicando no botão ***Remover***; a rede respetiva será então considerada desconhecida e possivelmente perigosa.

Nesta janela pode verificar quais são as redes que são consideradas redes conhecidas:



Nota: *a funcionalidade de redes conhecidas do Conselho do AVG não é compatível com o sistema operativo Windows XP de 64 bits.*

8. Definições da Firewall

A configuração da Firewall abre numa nova janela onde pode configurar, através de várias janelas, parâmetros avançados do componente. A configuração da Firewall abre numa nova janela onde pode editar os parâmetros avançados do componente em várias janelas de configuração. A configuração pode ser apresentada em modo básico ou em modo especializado. Quando acede pela primeira vez à janela de configuração, a janela é aberta na versão básica, que disponibiliza a edição dos seguintes parâmetros:

- Geral
- Aplicações
- Partilha de ficheiros e de impressoras

Na parte inferior da janela pode encontrar o botão ***Modo especializado***. Clique no botão para ver itens adicionais na navegação da janela, que possibilitam uma configuração muito avançada da Firewall:

- Definições Avançadas
- Redes definidas
- Serviços do Sistema
- Registos

8.1. Geral

A janela ***Informação geral*** apresenta uma síntese de todos os modos da Firewall disponíveis. O modo da Firewall que está selecionado pode ser alterado selecionando simplesmente outro modo no menu.

Tenha em atenção que o fornecedor do software configurou todos os componentes do AVG Internet Security para um desempenho otimizado. Não altere a configuração predefinida a menos que tenha uma razão imperativa para o fazer. Quaisquer alterações às definições deverão ser efetuadas exclusivamente por um utilizador avançado!

AVG Internet Security
Geral
Aplicações
Partilha de ficheiros e de impresso
Informação geral
Modo automático (recomendado)
A firewall permite ou bloqueia automaticamente as aplicações, dependendo do seu comportamento e da sua participação na base de dados interna de aplicações confiáveis.
Modo interativo
A firewall vai pedir para permitir o acesso ou bloquear todas as aplicações do seu computador.
Bloquear o acesso à Internet
A firewall bloqueia todas as tentativas de ligação para ou a partir da Internet.
Desligar a proteção da firewall (não recomendado)
A firewall não protege o seu computador em tudo. Permitir o tráfego de todas as aplicações.
Modo especializado
OK
Cancelar
Aplicar

A Firewall permite-lhe definir regras de segurança específicas consoante o seu computador esteja localizado num domínio, seja um computador independente ou mesmo um portátil. Cada uma destas opções requer um nível de proteção diferente, sendo os níveis abrangidos pelos respetivos modos. Resumindo, um modo da Firewall é uma configuração específica do componente Firewall, e pode usar uma variedade dessas configurações predefinidas:

- ***Automático*** – neste modo, a Firewall lida com todo o tráfego de rede automaticamente. O utilizador não terá de tomar qualquer decisão. A Firewall permitirá a ligação para cada aplicação conhecida e, ao mesmo tempo, será criada uma regra para a aplicação que especifica que a aplicação pode sempre estabelecer ligação no futuro. No caso de outras aplicações, a Firewall decide se a ligação deve ser permitida ou bloqueada com base no comportamento da aplicação. No entanto, numa situação desse tipo, a regra não será criada e a aplicação será verificada novamente quando tentar estabelecer ligação. ***O modo automático é extremamente discreto e é o modo recomendado para a maioria dos utilizadores.***

- ***Interativo*** – este modo é útil se pretender ter controlo total sobre todo o tráfego de rede que entra e sai do computador. A Firewall monitorizará o tráfego e avisá-lo-á se houver qualquer tentativa de comunicação ou transferência de dados, podendo depois permitir ou bloquear a tentativa conforme necessário. Recomendado apenas a utilizadores avançados.

- ***Bloquear o acesso à Internet*** – a ligação à Internet é totalmente bloqueada; deixa de poder aceder à Internet e ninguém do exterior pode aceder ao computador. Apenas para uso especial e de tempo limitado.

- ***Desligar a proteção da firewall*** – desativar a Firewall possibilitará o fluxo de todo o tráfego de rede do e para o computador. Consequentemente, o computador ficará mais vulnerável a ataques de piratas informáticos. Pense bem antes de selecionar esta opção.

Tenha em consideração um modo automático específico que também está disponível na Firewall. Esse modo é ativado silenciosamente se o componente Computador ou Proteção de Identidade for desativado e se o computador ficar mais vulnerável como consequência desse facto. Nesses casos, a Firewall permitirá

automaticamente apenas aplicações conhecidas e totalmente seguras. Ser-lhe-á pedida uma decisão no que diz respeito a todas as outras aplicações. Esta medida destina-se a compensar a proteção desativada e a manter o seu computador protegido.

8.2. Aplicações

A janela de ***Aplicações*** apresenta todas as aplicações que tentaram comunicar através da rede até ao momento e os ícones relativos à ação atribuída:

As aplicações na ***Lista de aplicações*** são as que foram detetadas no computador (*e às quais foram atribuídas ações respetivas*). Podem ser usados os seguintes tipos de ação:

- – permitir a comunicação para todas as redes
- – bloquear a comunicação
- – definições avançadas definidas

Tenha em atenção que só é possível detetar aplicações que já estejam instaladas. Por predefinição, quando uma nova aplicação tenta estabelecer ligação através da rede pela primeira vez, a Firewall cria uma nova regra automaticamente em conformidade com a base de dados segura ou pergunta ao utilizador se pretende permitir ou bloquear a comunicação. Na última situação, o utilizador poderá guardar a sua resposta como uma regra permanente (que ficará depois listada nesta janela).

Obviamente, também pode definir regras para a nova aplicação imediatamente – nesta janela, clique em ***Adicionar*** e preencha os detalhes da aplicação.

Para além das aplicações, a lista também contém dois itens especiais. ***Regras Prioritárias da Aplicação*** (*no topo da lista*) são preferenciais e são sempre aplicadas antes das regras de qualquer aplicação individual. ***Regras de Outras aplicações*** (*no fundo da lista*) são usadas como "último recurso", quando nenhuma regra

específica de aplicação for aplicável, ex. para uma aplicação desconhecida e indefinida. Selecione a ação que deve ser efetuada quando uma aplicação desse tipo tentar comunicar através da rede: Bloquear *(a comunicação será sempre bloqueada)*, Permitir *(a comunicação será permitida através de qualquer rede)*, Perguntar *(o utilizador poderá decidir se a comunicação deve ser permitida ou bloqueada)*. ***Estes itens têm opções de configuração diferentes das aplicações comuns, e são destinados exclusivamente a utilizadores experientes. Recomendamos vivamente que não modifique estas definições!***

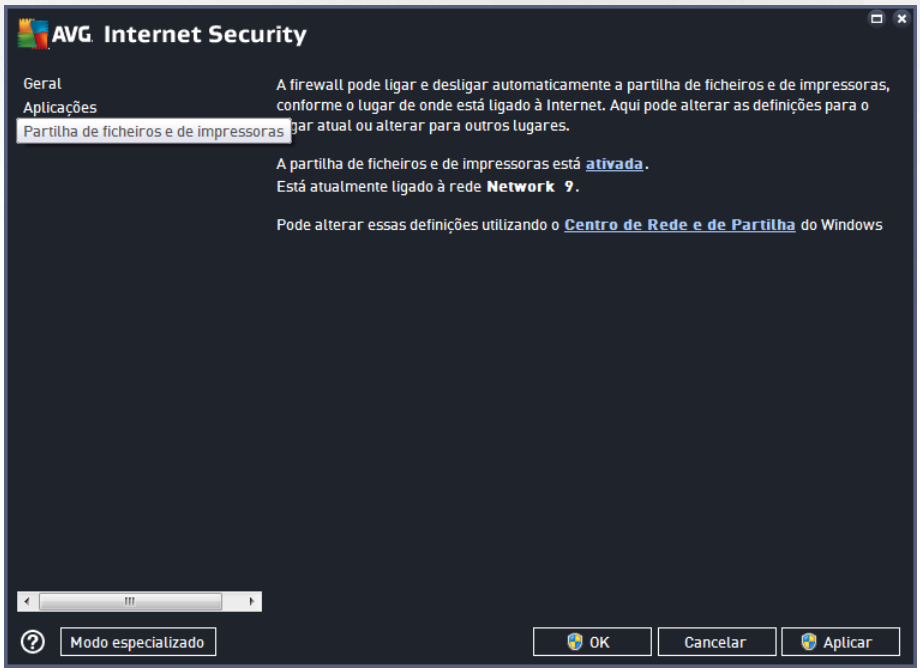
Botões de controlo

A lista pode ser editada usando os seguintes botões de controlo:

- ***Adicionar*** – abre uma janela em branco para definição de novas regras de aplicações.
- ***Editar*** – abre a mesma janela com dados disponibilizados para edição do conjunto de regras de uma aplicação existente.
- ***Eliminar*** – remove a aplicação selecionada da lista.

8.3. Partilha de ficheiros e de impressoras

Partilha de ficheiros e de impressoras significa, efetivamente, partilhar ficheiros ou pastas que sejam assinalados como "Partilhados" no Windows, em unidades de disco comuns, impressoras, digitalizadores e dispositivos semelhantes. A partilha desses itens só deverá ser feita dentro de redes que possam ser consideradas seguras *(por exemplo, em casa, no trabalho ou na escola)*. No entanto, se estiver ligado a uma rede pública *(como a rede Wi-Fi de um aeroporto ou um café com Internet)*, poderá não ser aconselhável partilhar seja o que for. A Firewall do AVG pode facilmente permitir ou bloquear a partilha e permite-lhe guardar a sua escolha para redes já visitadas.

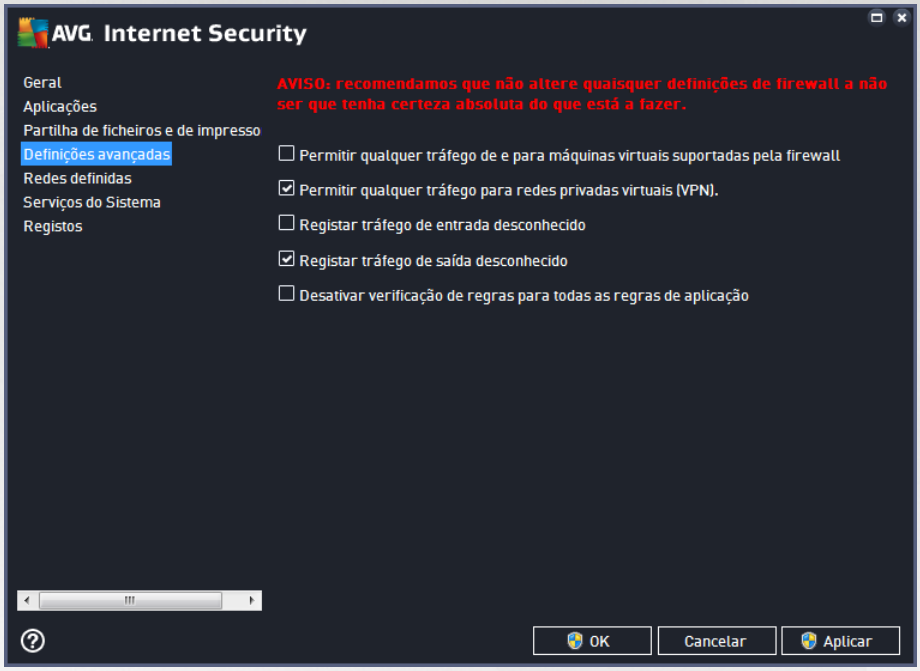

AVG. Internet Security
Geral
Aplicações
Partilha de ficheiros e de impressoras
A firewall pode ligar e desligar automaticamente a partilha de ficheiros e de impressoras, conforme o lugar de onde está ligado à Internet. Aqui pode alterar as definições para o
ar atual ou alterar para outros lugares.
A partilha de ficheiros e de impressoras está ativada.
Está atualmente ligado à rede Network 9.
Pode alterar essas definições utilizando o Centro de Rede e de Partilha do Windows
Modo especializado
OK
Cancelar
Aplicar

Na janela ***Partilha de ficheiros e de impressoras*** pode editar a configuração da partilha de ficheiros e impressoras, e as redes às quais o computador está ligado. No sistema operativo Windows XP, o nome da

rede corresponde à designação selecionada para a rede específica aquando da primeira ligação do computador à rede. No sistema operativo Windows Vista ou superior, o nome da rede é retirado automaticamente do Centro de Rede e Partilha.

8.4. Definições avançadas

A edição de itens na janela Definições avançadas destina-se APENAS A UTILIZADORES EXPERIENTES!


AVG Internet Security
Geral
Aplicações
Partilha de ficheiros e de impresso
Definições avançadas
Redes definidas
Serviços do Sistema
Registos
AVISO: recomendamos que não altere quaisquer definições de firewall a não ser que tenha certeza absoluta do que está a fazer.
Permitir qualquer tráfego de e para máquinas virtuais suportadas pela firewall
Permitir qualquer tráfego para redes privadas virtuais (VPN).
Registar tráfego de entrada desconhecido
Registar tráfego de saída desconhecido
Desativar verificação de regras para todas as regras de aplicação
OK
Cancelar
Aplicar

A janela ***Definições avançadas*** permite-lhe ativar/desativar os seguintes parâmetros da Firewall:

- ***Permitir qualquer tráfego de e para máquinas virtuais suportadas pela firewall*** – suporte para ligação de rede em máquinas virtuais (por exemplo, VMware).
- ***Permitir qualquer tráfego para redes privadas virtuais (VPN)*** – suporte para ligações de VPN *(utilizadas para estabelecer ligação a computadores remotos)*.
- ***Registar tráfego de entrada/saída desconhecido*** – todas as tentativas de comunicação *(entrada/saída)* efetuadas por aplicações desconhecidas serão gravadas no Registo da Firewall.
- ***Desativar verificação de regras para as regras de todas as aplicações*** – a Firewall monitoriza continuamente todos os ficheiros abrangidos por cada regra de uma aplicação. Quando ocorre uma modificação no ficheiro binário, a Firewall tenta novamente confirmar a credibilidade da aplicação por meios normais, ou seja, verificando o certificado da aplicação, procurando a aplicação na base de dados de aplicações fidedignas, etc. Se não for possível considerar a aplicação segura, a Firewall irá lidar com a aplicação consoante o modo selecionado:
  - se a Firewall for executada no ***modo Automático***, a aplicação será permitida por predefinição;
  - se a Firewall for executada no ***modo Interativo***, a aplicação será bloqueada e aparecerá uma caixa de diálogo a perguntar ao utilizador o que pretende fazer em relação à aplicação.

O procedimento utilizado para lidar com uma aplicação específica pode ser definido para cada aplicação na caixa de diálogo Aplicações.

8.5. Redes definidas

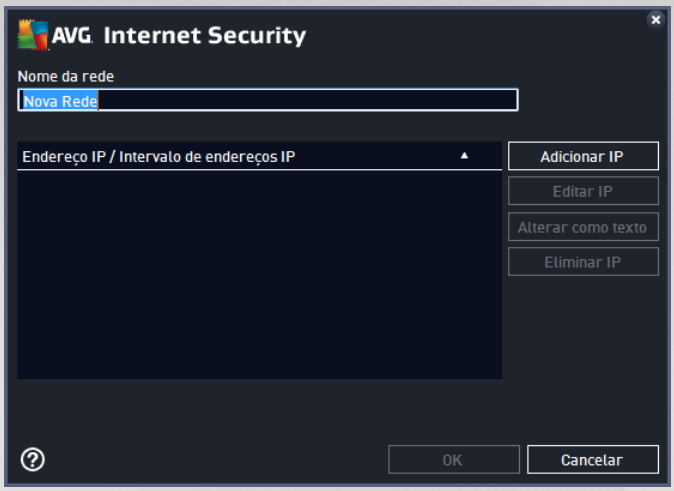
A edição de itens na janela Redes definidas destina-se APENAS A UTILIZADORES EXPERIENTES!

A janela ***Redes definidas*** faculta uma lista de todas as redes às quais o seu computador está ligado. A lista apresenta as seguintes informações relativas a cada rede detetada:

- ***Redes*** – apresenta uma lista de nomes de todas as redes às quais o computador está ligado.
- ***Intervalo de endereços IP*** – cada rede será detetada automaticamente e especificada sob a forma de intervalos de endereços IP.

Botões de controlo

- ***Adicionar rede*** – abre uma nova janela na qual pode editar os parâmetros da rede definida, ou seja, disponibilizar o ***Nome da rede*** e especificar o ***Intervalo de endereços IP***:

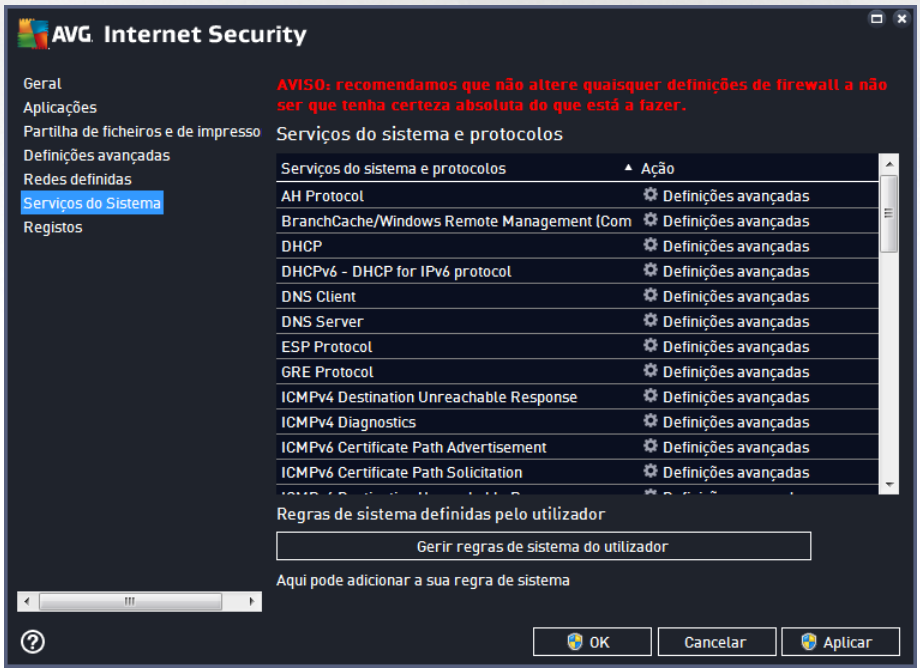


- ***Editar rede*** – abre a janela ***Propriedades de rede*** (*ver acima*), na qual pode editar os parâmetros de uma rede já definida (*a janela é idêntica à janela para adicionar novas redes, consulte a descrição no parágrafo anterior*).

- ***Eliminar rede*** – remove a referência a uma rede selecionada da lista de redes.

8.6. Serviços do Sistema

A edição de itens na janela Serviços do sistema e protocolos destina-se APENAS A UTILIZADORES EXPERIENTES!



A janela ***Serviços do sistema e protocolos*** lista os serviços de sistema e protocolos padrão do Windows que possam precisar de comunicar através da rede. A tabela é composta por duas colunas:

- ***Serviços do sistema e protocolos*** – Esta coluna apresenta o nome do serviço de sistema respetivo.

- ***Ação*** – Esta coluna apresenta um ícone para a ação atribuída:
    - o Permitir a comunicação para todas as redes
    - o Bloquear a comunicação

Para editar qualquer item da lista (*incluindo as ações atribuídas*), clique com o botão direito do rato e selecione ***Editar***. ***No entanto, a edição de regras do sistema deve ser efetuada exclusivamente por utilizadores avançados e é vivamente recomendável não editar as regras do sistema!***

Regras de sistema definidas pelo utilizador

Para abrir uma nova janela para definição das suas próprias regras do serviço do sistema (*consulte a imagem abaixo*), clique no botão ***Gerir regras de sistema do utilizador***. É aberta a mesma janela se optar por editar a configuração de qualquer um dos itens existentes na lista de serviços do sistema e protocolos. A secção superior da janela apresenta um resumo de todos os detalhes da regra de sistema atualmente em edição; a parte inferior apresenta o detalhe selecionado. É possível editar, adicionar ou eliminar os detalhes de uma regra utilizando o botão respetivo:

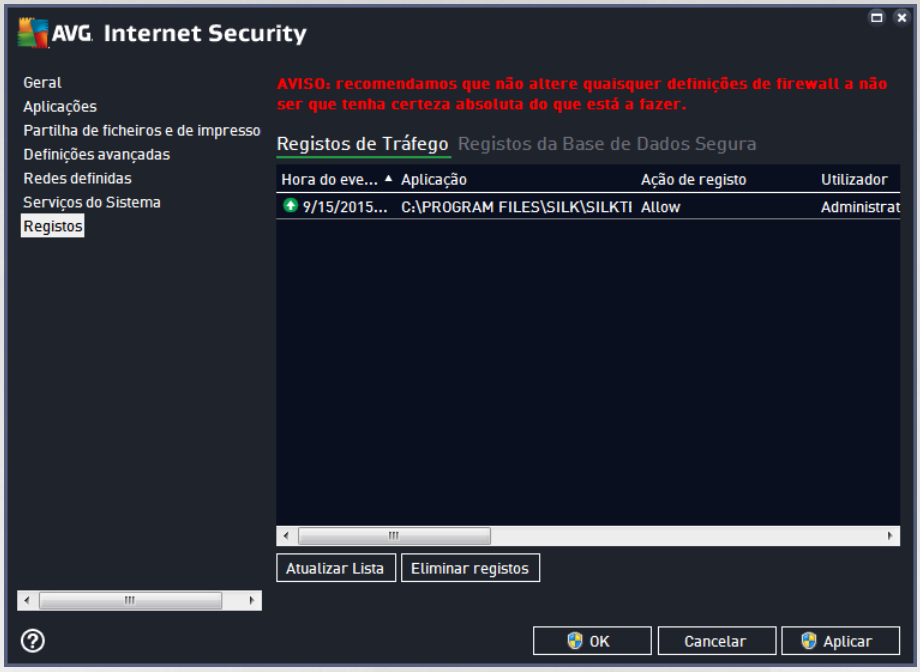
Tenha em atenção que as definições de detalhes de regras são avançadas e destinadas principalmente a administradores de redes que precisam de ter controlo absoluto sobre a configuração da Firewall. Se não estiver familiarizado com tipos de protocolos de comunicação, números de portas de rede, definições de endereços IP, etc., não modifique estas definições! Se precisar realmente de alterar a configuração, consulte os ficheiros de ajuda da janela respetiva para obter informações específicas.

8.7. Registos

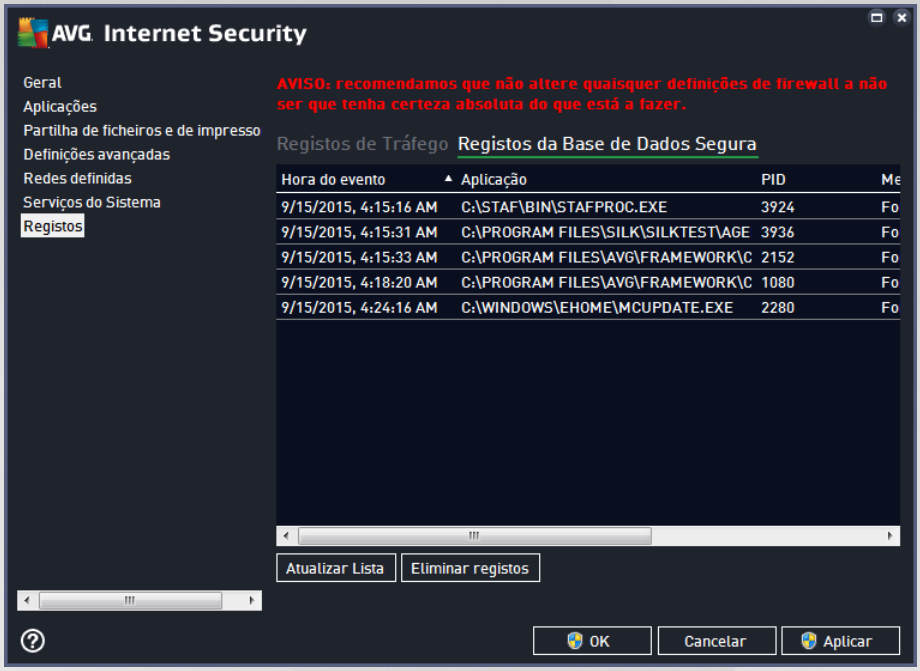
A edição de itens na janela Registos destina-se APENAS A UTILIZADORES EXPERIENTES!

A janela ***Registos*** permite-lhe rever a lista de todas as ações e eventos da Firewall com uma descrição detalhada de parâmetros relevantes, apresentados em dois separadores:

- ***Registos de Tráfego*** – Este separador apresenta informações relativas às atividades de todas as aplicações que tentaram estabelecer ligação à rede. Para cada item poderá encontrar informações relativas à hora do evento, o nome da aplicação, a ação de registo respetiva, o nome do utilizador, PID, direção do tráfego, tipo de protocolo, os números da porta remota e da porta local e informações relativas ao endereço IP remoto e local.



- ***Registos da Base de Dados Segura*** – A *Base de Dados Segura* é a base de dados interna do AVG que recolhe informações sobre aplicações certificadas e seguras que podem ter sempre permissão para comunicar online. Da primeira vez que uma nova aplicação tentar estabelecer ligação à rede (*ou seja, quando ainda não existe nenhuma regra da firewall especificada para essa aplicação*), é necessário descobrir se a comunicação na rede deve ser permitida para a respetiva aplicação. Primeiro, o AVG procura na *Base de Dados Segura* e, se a aplicação estiver listada, ser-lhe-á concedido acesso à rede automaticamente. Só depois disso, se não houver qualquer informação sobre a aplicação disponível na base de dados, será o utilizador inquirido, por meio de uma janela independente, sobre se pretende que a aplicação aceda à rede.



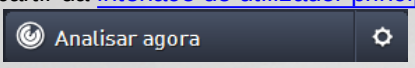
Botões de controlo

- ***Atualizar lista*** – todos os parâmetros registados podem ser ordenados consoante o atributo selecionado: cronologicamente (*datas*) ou alfabeticamente (*outras colunas*) – basta clicar no cabeçalho da coluna respetiva. Utilize o botão ***Atualizar lista*** para atualizar a informação apresentada.

- ***Eliminar registos*** – clique para eliminar todas as entradas da tabela.

9. Análise do AVG

Por predefinição, o **AVG Internet Security** não executa qualquer análise, uma vez que, após a análise inicial *(que o utilizador será convidado a iniciar*), o utilizador deverá ficar devidamente protegido pelos componentes residentes do **AVG Internet Security** que estão sempre alerta e não permitem que nenhum código malicioso aceda ao computador. Obviamente, o utilizador pode agendar uma análise para execução a intervalos regulares, ou iniciar uma análise manualmente consoante as necessidades pontuais.

É possível aceder à interface de análise do AVG a partir da interface de utilizador principal através do botão que, graficamente, está dividido em duas secções: 

- ***Analisar agora*** – Clique neste botão para iniciar de imediato a operação Analisar todo o computador e veja o progresso e os resultados na janela Relatórios que é aberta automaticamente:

- ***Opções*** – Selecione este botão *(apresentado graficamente sob a forma de três linhas horizontais num fundo verde)* para abrir a janela ***Opções de análise***, na qual pode gerir análises agendadas e editar parâmetros de Analisar todo o computador / Analisar pastas ou ficheiros.

Na janela ***Opções de análise***, pode ver três secções principais de configuração de análises:

- ***Gerir análises agendadas*** – Clique nesta opção para abrir uma nova janela com uma síntese de todas as análises agendadas. Antes de definir análises personalizadas, só verá na tabela uma análise agendada predefinida pelo fornecedor do software. A análise está desativada por predefinição. Para ativar a análise, clique com o botão direito do rato na mesma e selecione a opção *Ativar tarefa* no menu de contexto. Depois de ativar a análise agendada, poderá editar a respetiva configuração através do botão *Editar análise agendada*. Também pode clicar no botão *Adicionar análise agendada* para criar uma nova análise agendada.

- ***Analisar todo o computador / Definições*** – O botão está dividido em duas secções. Clique na opção *Analisar todo o computador* para iniciar de imediato a análise de todo o computador *(para mais informações sobre a análise de todo o computador, consulte o respetivo capítulo com o título Análises Predefinidas / Analisar todo o computador)*. Se clicar na secção *Definições*, poderá aceder à janela de configuração da análise de todo o computador.

- ***Analisar pastas ou ficheiros / Definições*** – Mais uma vez, o botão está dividido em duas secções. Clique na opção *Analisar pastas ou ficheiros* para iniciar de imediato a análise de áreas selecionadas do computador *(para mais informações sobre a análise de pastas ou ficheiros selecionados, consulte o respetivo capítulo com o título Análises Predefinidas / Analisar pastas ou ficheiros)*. Se clicar na secção *Definições*, poderá aceder à janela de configuração da análise de pastas ou ficheiros.

- ***Analisar o computador para procurar rootkits / Definições*** – A secção esquerda do botão identificado como *Analisar o computador para procurar rootkits* inicia de imediato a análise anti-rootkit *(para mais informações sobre a análise de rootkits, consulte o respetivo capítulo com o título Análises Predefinidas / Analisar o computador para procurar rootkits)*. Se clicar na secção *Definições*, poderá aceder à janela de configuração da análise de rootkits.

9.1. Análises Predefinidas

Uma das principais funcionalidades do **AVG Internet Security** é a análise manual. Os testes a pedido são concebidos para analisar várias partes do computador sempre que existam suspeitas de uma possível infeção por vírus. De qualquer modo, recomenda-se vivamente que esses testes sejam efetuados regularmente,

mesmo que considere que não serão detetados vírus no computador.

No **AVG Internet Security** encontrará os seguintes tipos de análises predefinidas pelo fornecedor do software:

9.1.1. Analisar todo o computador

Analisar todo o computador analisa todo o computador para procurar possíveis infeções e/ou aplicações potencialmente indesejadas. Este teste analisará todos os discos rígidos no seu computador, detetará e recuperará qualquer vírus encontrado ou removerá a infeção detetada para a Quarentena de Vírus. A análise de todo o computador deve ser agendada no computador pelo menos uma vez por semana.

Início de análise

A análise ***Analisar todo o computador*** pode ser iniciada diretamente na interface de utilizador principal clicando no botão ***Analisar agora***. Não é necessário configurar definições específicas adicionais para este tipo de análise; a análise é iniciada de imediato. Na janela ***Analisar todo o computador em execução*** (*consulte a captura de ecrã*), pode ver o progresso e os resultados da análise. A análise pode ser temporariamente interrompida (***Interromper***) ou cancelada (***Parar***) se necessário.

Edição da configuração de análise

Pode editar a configuração de ***Analisar todo o computador*** na janela ***Analisar todo o computador – Definições*** (*pode aceder à janela através da ligação Definições de Analisar todo o computador na janela Opções de análise*). ***É recomendável que mantenha as predefinições a menos que tenha uma razão válida para as alterar!***

AVG Internet Security
Analisar todo o computador - Definições
Recuperar/remover infeções causadas por vírus sem me perguntar
Reportar a existência de aplicações potencialmente indesejadas e ameaças de spyware
Reportar conjunto avançado de aplicações potencialmente indesejadas
Analisar Cookies de Rastreio
Pesquisa no interior dos arquivos
Utilizar Heurística
Analisar ambiente de sistema
Ativar análise minuciosa
Analisar rootkits
Ajustar a rapidez de conclusão de uma Análise
Opção do utilizador
Definições de análise adicionais
Definir relatórios de análise adicionais
Predefinição
Guardar as definições atuais
Iniciar análise
compilação 7132

Na lista de parâmetros de análise pode ativar/desativar parâmetros específicos consoante necessário:

- ***Recuperar/remover infeções causadas por vírus sem me perguntar*** *(ativado por predefinição)* – Se um vírus for detetado durante a análise, pode ser recuperado automaticamente se houver uma cura disponível. Se não for possível recuperar o ficheiro infetado automaticamente, o objeto infetado será movido para a Quarentena de Vírus.

- ***Reportar aplicações potencialmente indesejadas e ameaças de spyware*** *(ativado por predefinição)* – Marque esta opção para ativar a análise que procura spyware e também vírus. O Spyware representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade ativada, uma vez que aumenta a segurança do seu computador.

- ***Reportar conjunto avançado de aplicações potencialmente indesejadas*** *(desativado por predefinição)* – Marque esta opção para detetar pacotes expandidos de spyware: programas que são perfeitamente fidedignos e inofensivos quando adquiridos diretamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, poderá bloquear programas legais e está, como tal, desativada por predefinição.

- ***Analisar Cookies de Rastreio*** *(desativado por predefinição)* – Este parâmetro especifica que os cookies deverão ser detetados *(os cookies HTTP são utilizados para autenticação, rastreio e manutenção de informação específica dos utilizadores, tal como preferências de websites ou os conteúdos dos carrinhos de compras eletrónicos dos mesmos)*.

- ***Pesquisa no interior dos arquivos*** *(desativado por predefinição)* – Este parâmetro especifica que a análise deve verificar todos os ficheiros guardados em arquivos, ex.: ZIP, RAR, etc.

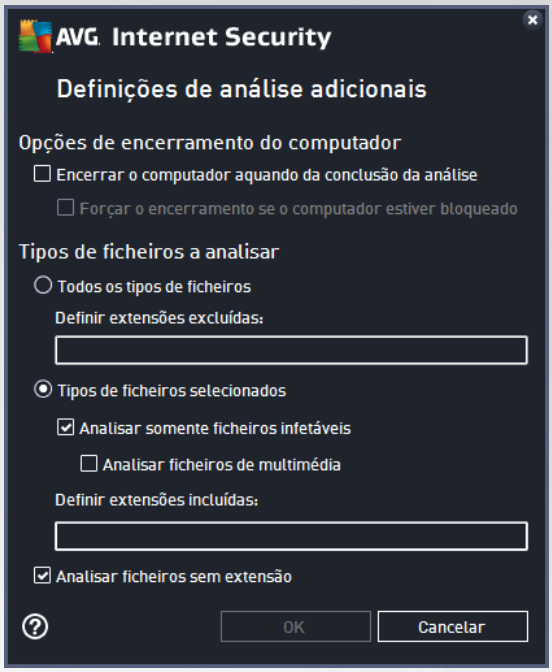
- ***Utilizar Heurística*** *(ativado por predefinição)* – A análise heurística *(emulação dinâmica das instruções do objeto analisado num ambiente de computador virtual)* será um dos métodos utilizados para a deteção de vírus durante a análise.

- ***Analisar ambiente de sistema*** *(ativado por predefinição)* – A análise verificará também as áreas de sistema do seu computador.

- ***Ativar análise minuciosa*** *(desativado por predefinição)* – Em situações específicas *(suspeitas de infeção do computador)* pode marcar esta opção para ativar os algoritmos de análise mais rigorosos que irão analisar todas as áreas do seu computador, incluindo as que raramente são infetadas, por precaução. Tenha em consideração que este método é bastante demorado.

- ***Analisar rootkits*** *(ativado por predefinição)*: inclui a análise anti-rootkit na análise de todo o computador. A análise anti-rootkit também pode ser iniciada separadamente.

- ***Definições de análise adicionais*** – a ligação abre uma nova janela de Definições de análise adicionais onde pode especificar os seguintes parâmetros:


AVG. Internet Security
Definições de análise adicionais
Opções de encerramento do computador
Encerrar o computador aquando da conclusão da análise
Forçar o encerramento se o computador estiver bloqueado
Tipos de ficheiros a analisar
Todos os tipos de ficheiros
Definir extensões excluídas:
Tipos de ficheiros selecionados
Analisar somente ficheiros infetáveis
Analisar ficheiros de multimédia
Definir extensões incluídas:
Analisar ficheiros sem extensão
OK
Cancelar

  - ***Opções de encerramento do computador*** – decida se o computador deve ser encerrado automaticamente uma vez concluído o processo de análise em execução. Tendo confirmado esta opção (***Encerrar o computador aquando da conclusão da análise***), será ativada uma nova opção que permite que o computador encerre mesmo que esteja bloqueado (***Forçar o encerramento se o computador estiver bloqueado***).

  - ***Tipos de ficheiros a analisar*** – também deve decidir se pretende analisar:

    - ***Todos os tipos de ficheiros*** com a opção de definir exceções da análise ao indicar uma lista de extensões separadas por vírgula que não devem ser analisadas;

    - ***Tipos de ficheiros selecionados*** – pode especificar que pretende analisar apenas ficheiros que possam ser infetados (*ficheiros que não possam ser infetados não serão analisados, por exemplo, alguns ficheiros de texto simples ou outros ficheiros não executáveis*), incluindo ficheiros multimédia (*ficheiros de áudio, vídeo – se deixar esta caixa desmarcada, reduzirá o tempo de análise ainda mais, uma vez que os ficheiros são por vezes muito grandes e é pouco provável que estejam infetados por vírus*). Mais uma vez, pode especificar por extensões os ficheiros que deverão ser sempre analisados.

    - Opcionalmente, pode decidir se pretende ***Analisar ficheiros sem extensão*** – esta opção

está ativada por predefinição e é recomendável que a mantenha assim a menos que tenha uma razão válida para a alterar. Os ficheiros sem extensões são bastante suspeitos e devem ser sempre analisados.

- ***Ajustar a rapidez de conclusão de uma Análise*** – pode utilizar o cursor para alterar a prioridade do processo de análise. Por predefinição, o valor desta opção está definido para o nível de *Opção do utilizador* de utilização automática de recursos. Em alternativa, pode executar o processo de análise mais lentamente, o que significa que a utilização dos recursos do sistema será minimizada (*prático quando precisa de trabalhar no computador, mas não se preocupa com a duração da análise*), ou mais rapidamente com requisitos de recursos de sistema mais elevados (*por exemplo, quando o computador não está a ser utilizado*).

- ***Definir relatórios de análise adicionais*** – a ligação abre uma nova janela de ***Relatórios de análise*** onde pode selecionar que tipos de possíveis deteções deverão ser reportados:

Aviso: *estas definições de análise são idênticas aos parâmetros de uma análise nova, conforme descrito no capítulo Análise do AVG / Agendamento de análises / Como analisar. Na eventualidade de decidir alterar a configuração predefinida da análise* ***Analisar todo o computador****, pode guardar as suas novas definições como a configuração predefinida a ser utilizada para todas as análises de todo o computador.*

9.1.2. Analisar pastas ou ficheiros

Analisar pastas ou ficheiros – analisa apenas as áreas do computador que tiver selecionado para o efeito (*pastas selecionadas, discos rígidos, unidades de disquetes, CDs, etc.*). O progresso da análise na eventualidade de deteção de vírus e o seu tratamento é o mesmo que o da análise de todo o computador: qualquer vírus detetado é recuperado ou removido para a Quarentena de Vírus. A análise de ficheiros ou pastas específicos pode ser utilizada para configurar os seus próprios testes e os seus agendamentos consoante as suas necessidades.

Início de análise

A ***Análise de ficheiros/pastas*** pode ser iniciada diretamente na janela Opções de análise clicando no botão **Analisar pastas ou ficheiros**. Será apresentada uma nova janela intitulada ***Selecionar ficheiros ou pastas específicos a analisar***. Na estrutura em árvore do seu computador selecione as pastas que pretende analisar. O caminho para cada pasta será gerado automaticamente e aparecerá na caixa de texto na parte superior da janela. Também existe a opção de analisar uma pasta específica excluindo todas as subpastas da análise; para isso deverá escrever um sinal de menos "**-**" antes do caminho gerado automaticamente (*consulte a captura de ecrã*). Para excluir toda a pasta da análise utilize o parâmetro "!". Finalmente, para iniciar a análise, clique no botão ***Iniciar análise***; o processo de análise em si é praticamente idêntico ao de Analisar

todo o computador.

Edição da configuração de análise

Pode editar a configuração de ***Analisar pastas ou ficheiros*** na janela ***Analisar pastas ou ficheiros – Definições*** *(pode aceder à janela através da ligação Definições de Analisar pastas ou ficheiros na janela Opções de análise)*. ***É recomendável que mantenha as predefinições a menos que tenha uma razão válida para as alterar!***

AVG Internet Security
Analisar pastas ou ficheiros - Definições
Recuperar/remover infeções causadas por vírus sem me perguntar
Reportar a existência de aplicações potencialmente indesejadas e ameaças de spyware
Reportar conjunto avançado de aplicações potencialmente indesejadas
Analisar Cookies de Rastreio
Pesquisa no interior dos arquivos
Utilizar Heurística
Analisar ambiente de sistema
Ativar análise minuciosa
Ajustar a rapidez de conclusão de uma Análise
Opção do utilizador
Definições de análise adicionais
Definir relatórios de análise adicionais
Predefinição
Guardar as definições atuais
Seguinte
compilação 7132

Na lista de parâmetros de análise, pode ativar/desativar parâmetros específicos conforme necessário:

- ***Recuperar/remover infeções causadas por vírus sem me perguntar*** *(ativado por predefinição)*: se um vírus for detetado durante a análise, pode ser recuperado automaticamente se houver uma cura disponível. Se não for possível recuperar o ficheiro infetado automaticamente, o objeto infetado será

movido para a Quarentena de Vírus.

- ***Reportar aplicações potencialmente indesejadas e ameaças de spyware*** *(ativado por predefinição)*: marque esta opção para ativar a análise que procura spyware e também vírus. O Spyware representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade ativada, uma vez que aumenta a segurança do seu computador.

- ***Reportar conjunto avançado de aplicações potencialmente indesejadas*** *(desativado por predefinição)*: marque esta opção para detetar pacotes expandidos de spyware: programas que são perfeitamente fidedignos e inofensivos quando adquiridos diretamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, poderá bloquear programas legais e está, como tal, desativada por predefinição.

- ***Analisar Cookies de Rastreio*** *(desativado por predefinição)*: este parâmetro especifica que os cookies deverão ser detetados *(os cookies HTTP são utilizados para autenticação, rastreio e manutenção de informação específica dos utilizadores, tal como preferências de websites ou os conteúdos dos carrinhos de compras eletrónicos dos mesmos)*.

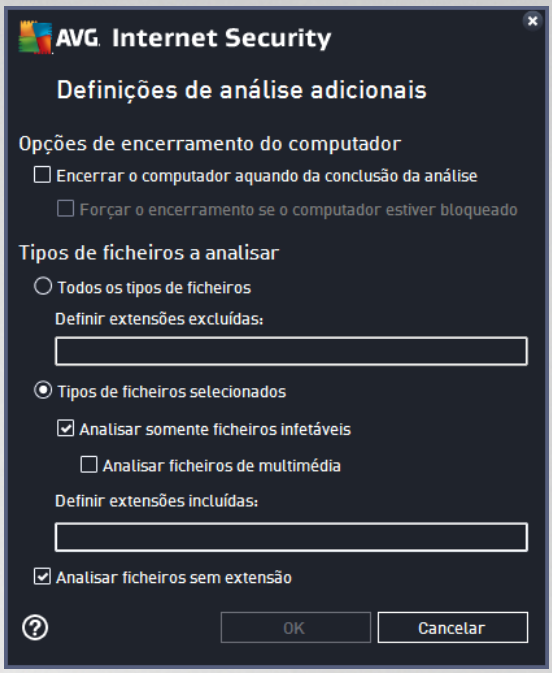
- ***Pesquisa no interior dos arquivos*** *(ativado por predefinição)*: este parâmetro define que a análise deve verificar todos os ficheiros guardados em arquivos, ex.: ZIP, RAR, etc.

- ***Utilizar Heurística*** *(ativado por predefinição)*: a análise heurística *(emulação dinâmica das instruções do objeto analisado num ambiente de computador virtual)* será um dos métodos utilizados para a deteção de vírus durante a análise.

- ***Analisar ambiente de sistema*** *(desativado por predefinição)*: a análise verificará também as áreas de sistema do seu computador.

- ***Ativar análise minuciosa*** *(desativado por predefinição)*: em situações específicas *(suspeitas de infeção do computador)* pode marcar esta opção para ativar os algoritmos de análise mais rigorosos que irão analisar todas as áreas do seu computador, incluindo as que raramente são infetadas, por precaução. Tenha em consideração que este método é bastante demorado.

- ***Definições de análise adicionais*** – A ligação abre uma nova janela de ***Definições de análise adicionais*** onde pode especificar os seguintes parâmetros:


AVG Internet Security
Definições de análise adicionais
Opções de encerramento do computador
Encerrar o computador aquando da conclusão da análise
Forçar o encerramento se o computador estiver bloqueado
Tipos de ficheiros a analisar
Todos os tipos de ficheiros
Definir extensões excluídas:
Tipos de ficheiros selecionados
Analisar somente ficheiros infetáveis
Analisar ficheiros de multimédia
Definir extensões incluídas:
Analisar ficheiros sem extensão
OK
Cancelar

- ***Opções de encerramento do computador*** – decida se o computador deve ser encerrado automaticamente uma vez concluído o processo de análise em execução. Tendo confirmado esta opção (***Encerrar o computador aquando da conclusão da análise***), será ativada uma nova opção que permite que o computador encerre mesmo que esteja bloqueado (***Forçar o encerramento se o computador estiver bloqueado***).

- ***Tipos de ficheiros a analisar*** – também deve decidir se pretende analisar:

  - ***Todos os tipos de ficheiros*** com a opção de definir exceções da análise ao indicar uma lista de extensões separadas por vírgula que não devem ser analisadas;

  - ***Tipos de ficheiros selecionados*** – pode especificar que pretende analisar apenas ficheiros que possam ser infetados (*ficheiros que não possam ser infetados não serão analisados, por exemplo, alguns ficheiros de texto simples ou outros ficheiros não executáveis*), incluindo ficheiros multimédia (*ficheiros de áudio, vídeo – se deixar esta caixa desmarcada, reduzirá o tempo de análise ainda mais, uma vez que os ficheiros são por vezes muito grandes e é pouco provável que estejam infetados por vírus*). Mais uma vez, pode especificar por extensões os ficheiros que deverão ser sempre analisados.

  - Opcionalmente, pode decidir se pretende ***Analisar ficheiros sem extensão*** – esta opção está ativada por predefinição e é recomendável que a mantenha assim a menos que tenha uma razão válida para a alterar. Os ficheiros sem extensões são bastante suspeitos e devem ser sempre analisados.

- ***Ajustar a rapidez de conclusão de uma Análise*** – pode utilizar o cursor para alterar a prioridade do processo de análise. Por predefinição, o valor desta opção está definido para o nível de *Opção do utilizador* de utilização automática de recursos. Em alternativa, pode executar o processo de análise mais lentamente, o que significa que a utilização dos recursos do sistema será minimizada (*prático quando precisa de trabalhar no computador, mas não se preocupa com a duração da análise*), ou mais rapidamente com requisitos de recursos de sistema mais elevados (*por exemplo, quando o computador não está a ser utilizado*).

- ***Definir relatórios de análise adicionais*** – a ligação abre uma nova janela de ***Relatórios de análise*** onde pode selecionar que tipos de possíveis deteções deverão ser reportados:

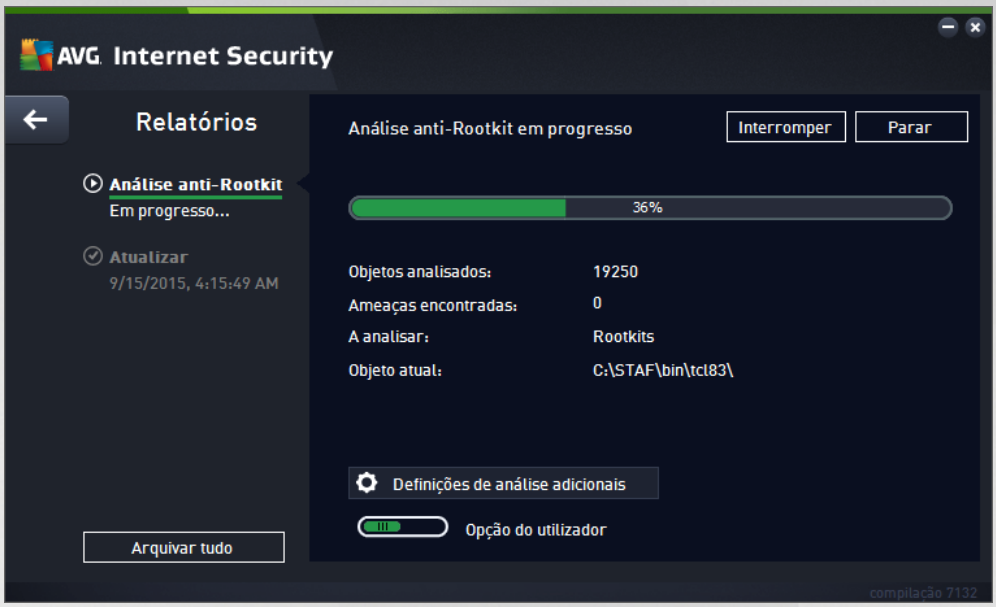
Aviso: *estas definições de análise são idênticas aos parâmetros de uma análise nova, conforme descrito no capítulo Análise do AVG / Agendamento de análises / Como analisar. Na eventualidade de decidir alterar a configuração predefinida da análise* ***Analisar pastas ou ficheiros****, pode guardar as suas novas definições como a configuração predefinida a ser utilizada para todas as análises de ficheiros e pastas específicos. Além disso, esta configuração será utilizada como modelo para todos os novos agendamentos de análise (todas as análises personalizadas são baseadas na configuração atual da análise Analisar pastas ou ficheiros).*

9.1.3. Analisar o computador para procurar rootkits

Analisar o computador para procurar rootkits consiste em detetar e remover eficazmente rootkits perigosos, ou seja, programas e tecnologias que podem disfarçar a presença de software malicioso no computador. Um rootkit é concebido para assumir o controlo do sistema do computador, sem a autorização dos proprietários e gestores legítimos do mesmo. A análise consegue detetar rootkits com base num conjunto de regras previamente definidas. A deteção de um rootkit não significa necessariamente que o rootkit esteja infetado. Por vezes, os rootkits são usados como controladores ou como componentes de aplicações seguras.

Início de análise

A operação ***Analisar o computador para procurar rootkits*** pode ser iniciada diretamente na janela Opções de análise clicando no botão ***Analisar o computador para procurar rootkits***. Aparece uma nova janela com o nome ***Análise anti-Rootkit em progresso***, que mostra o progresso da análise iniciada:



Edição da configuração de análise

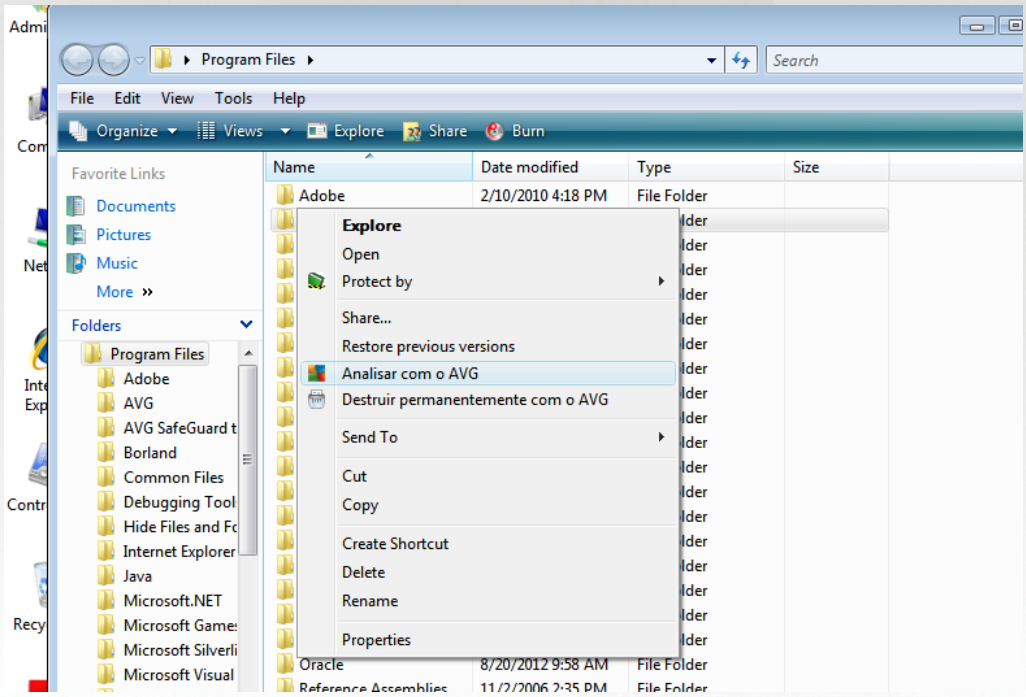
Pode editar a configuração da Análise anti-Rootkit na janela ***Definições de Anti-Rootkit*** *(pode aceder à janela através da ligação Definições de Analisar o computador para procurar rootkits na janela Opções de análise).* ***É recomendável que mantenha as predefinições a menos que tenha uma razão válida para as alterar!***

Analisar aplicações e ***Analisar controladores*** permitem-lhe especificar detalhadamente o que deve ser incluído na análise anti-rootkit. Estas definições são destinadas a utilizadores avançados; recomendamos que mantenha todas as opções ativadas. Também pode escolher o modo de análise de rootkits:

- ***Análise rápida de rootkits*** – analisa todos os processos em execução, todos os controladores carregados e também a pasta de sistema (*normalmente c:\Windows*)
- ***Análise completa de rootkits*** – analisa todos os processos em execução, todos os controladores carregados e também a pasta de sistema (*normalmente c:\Windows*), e todos os discos locais (*incluindo unidades flash, mas excluindo unidades de disquete/CD*)

9.2. Analisar no Explorador do Windows

Para além das análises predefinidas executadas para todo o computador ou as suas áreas selecionadas, o **AVG Internet Security** também disponibiliza a opção de análise rápida de um objeto específico diretamente no ambiente do Explorador do Windows. Se quiser abrir um ficheiro desconhecido e não estiver seguro do seu conteúdo, pode querer analisá-lo manualmente. Siga estes passos:



- No Explorador do Windows selecione o ficheiro *(ou pasta)* que pretende analisar
- Clique com o botão direito do rato no objeto para abrir o menu de contexto
- Selecione a opção ***Analisar com o AVG*** para proceder à análise do ficheiro com o **AVG Internet Security**

9.3. Análise da Linha de Comandos

No **AVG Internet Security** existe ainda a opção de executar a análise a partir da linha de comandos. Pode utilizar esta opção em servidores por exemplo, ou ao criar um batch script a ser executado automaticamente após o arranque do computador. Pode iniciar a análise a partir da linha de comandos com vários parâmetros, como na interface gráfica de utilizador do AVG.

Para iniciar a análise do AVG a partir da linha de comandos, execute o seguinte comando na pasta em que o AVG está instalado:

- ***avgscanx*** para SO de 32 bits
- ***avgscana*** para SO de 64 bits

Sintaxe do comando

A sintaxe do comando é a seguinte:

- ***avgscanx /parâmetro*** ... ex. ***avgscanx /comp*** para analisar todo o computador
- ***avgscanx /parâmetro /parâmetro*** .. com vários parâmetros, estes deverão estar alinhados numa linha e separados por espaço e o símbolo "barra"
- se um parâmetro requerer que seja facultado um valor específico (ex. o parâmetro ***/scan*** que requer informação relativa às áreas selecionadas do seu computador a serem analisadas, e o utilizador tiver de facultar a localização exata da secção selecionada), os valores são separados por ponto e vírgula, por exemplo: ***avgscanx /scan=C:\;D:***

Parâmetros de análise

Para visualizar uma síntese integral dos parâmetros disponíveis, digite o comando respetivo com o parâmetro /? ou /HELP (ex. ***avgscanx /?***). O único parâmetro obrigatório é /SCAN para especificar que áreas do computador devem ser analisadas. Para uma explicação mais detalhada das opções, consulte a síntese de parâmetros da linha de comandos.

Para executar a análise prima ***Enter***. Pode parar o processo durante a análise utilizando as combinações ***Ctrl +C*** ou ***Ctrl+Pause***.

Análise CMD iniciada a partir da interface gráfica

Ao iniciar o computador no Modo de Segurança do Windows, também existe a opção de iniciar a análise da linha de comandos a partir da interface gráfica de utilizador. A análise em si será iniciada a partir da linha de comandos, a janela ***Compositor de Linha de Comandos*** só permite especificar a maioria dos parâmetros de análise no conforto da interface gráfica.

Uma vez que esta janela só é acessível no Modo de Segurança do Windows, para uma descrição detalhada desta janela consulte o ficheiro de ajuda que pode ser aberto diretamente a partir da janela.

9.3.1. Parâmetros da Análise CMD

Segue-se uma lista de todos os parâmetros disponíveis para análises através da linha de comandos:

- /SCAN Analisar pastas ou ficheiros /SCAN=caminho;caminho *(ex.: /SCAN=C:\;D:\)*
- /COMP Analisar todo o computador
- /HEUR Utilizar análise heurística
- /EXCLUDE Excluir caminho ou ficheiros da análise

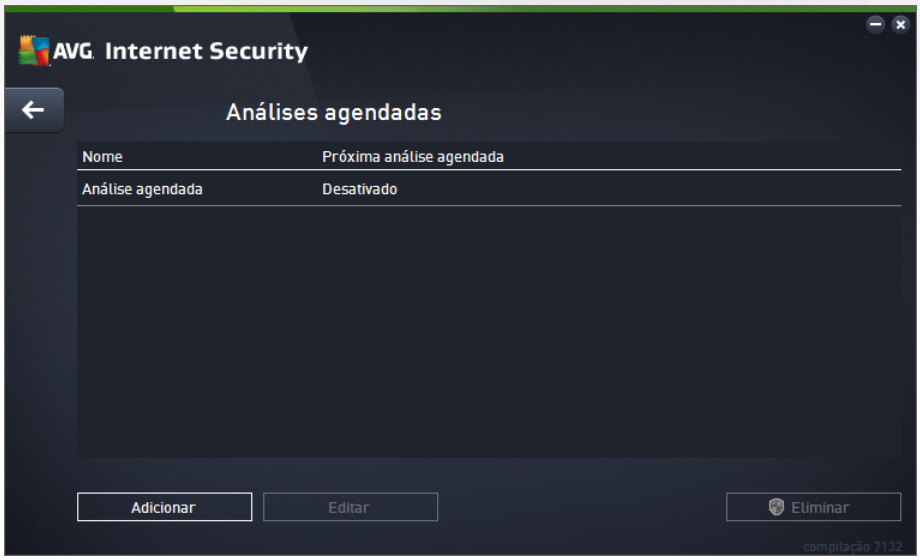
- /@ Ficheiro de comandos /nome de ficheiro/
- /EXT Analisar estas extensões /por exemplo EXT=EXE,DLL/
- /NOEXT Não analisar estas extensões /por exemplo NOEXT=JPG/
- /ARC Analisar arquivos
- /CLEAN Limpar automaticamente
- /TRASH Mover ficheiros infetados para a Quarentena de Vírus
- /QT Teste rápido
- /LOG Gerar um ficheiro com os resultados da análise
- /MACROW Reportar macros
- /PWDW Reportar ficheiros protegidos por palavra-passe
- /ARCBOMBSW Reportar bombas de arquivos *(arquivos comprimidos repetidamente)*
- /IGNLOCKED Ignorar ficheiros bloqueados
- /REPORT Reportar para ficheiro /nome de ficheiro/
- /REPAPPEND Anexar ao ficheiro de relatório
- /REPOK Reportar ficheiros não infetados como OK
- /NOBREAK Não permitir CTRL-BREAK para cancelar
- /BOOT Ativar verificação MBR/BOOT
- /PROC Analisar processos ativos
- /PUP Reportar aplicações potencialmente indesejadas
- /PUPEXT Reportar conjunto avançado de aplicações potencialmente indesejadas
- /REG Analisar registo
- /COO Analisar cookies
- /? Apresentar ajuda relativa a este tópico
- /HELP Apresentar ajuda relativa a este tópico
- /PRIORITY Definir a prioridade de análise /Baixa, Auto, Alta/ *(consulte a secção Definições avançadas / Análises)*
- /SHUTDOWN Encerrar o computador aquando da conclusão da análise

- /FORCESHUTDOWN Forçar o encerramento do computador aquando da conclusão da análise
- /ADS Analisar fluxos de dados alternativos *(apenas NTFS)*
- /HIDDEN Reportar ficheiros com extensões ocultas
- /INFECTABLEONLY Analisar apenas ficheiros com extensões infetáveis
- /THOROUGHSCAN Ativar análise minuciosa
- /CLOUDCHECK Verificar a existência de falsos positivos
- /ARCBOMBSW Reportar ficheiros de arquivo recomprimidos

9.4. Agendamento de Análise

Com o **AVG Internet Security** pode executar análises manualmente *(por exemplo, quando suspeita que uma infeção entrou no computador)* ou com base num agendamento planeado. É vivamente recomendável que execute as análises com base num agendamento: dessa forma pode assegurar que o seu computador está protegido de quaisquer possibilidades de ser infetado e não terá de se preocupar com quando e se iniciar uma análise. Deve executar a operação Analisar todo o computador regularmente, pelo menos uma vez por semana. No entanto, se possível, execute a análise de todo computador diariamente – conforme configurado na configuração de agendamento de análise predefinida. Se o computador estiver "sempre ligado", então pode agendar análises fora das horas de expediente. Se o computador for desligado ocasionalmente, então agende as análises para serem executadas no arranque do computador se não tiver sido possível efetuar a tarefa.

O agendamento da análise pode ser criado/editado na janela ***Análises agendadas***, à qual é possível aceder através do botão ***Gerir Análises Agendadas*** na janela Opções de análise. Na nova janela ***Análises agendadas*** pode ver uma síntese completa de todas as análises que estão agendadas:



Pode especificar análises personalizadas na janela. Utilize o botão ***Adicionar análise agendada*** para criar uma nova análise agendada. Os parâmetros da análise agendada podem ser editados (*ou pode ser configurado um novo agendamento*) em três separadores:

- Programar
- Definições
- Localização

Em cada separador, pode simplesmente clicar no botão de "semáforo" para desativar a análise agendada temporariamente e ativá-la novamente quando for necessário.

9.4.1. Programar

Na parte superior do separador ***Programar*** pode encontrar o campo de texto no qual pode especificar o nome da análise agendada que está a ser definida. Tente utilizar nomes curtos, descritivos e apropriados de análises para que futuramente seja mais fácil distinguir as análises de outras que venha a definir. Por exemplo, não é adequado nomear uma análise com o nome "Nova análise" ou "A minha análise" uma vez que estes nomes não referem o que a análise efetivamente analisa. Por outro lado, um exemplo de um bom nome descritivo seria "Análise das áreas de sistema", etc.

Nesta janela pode ainda definir os seguintes parâmetros de análise:

- ***Agendamento em execução*** – Aqui, pode especificar os intervalos de tempo para a execução da nova análise agendada. A temporização pode ser definida pela execução repetida da análise após um determinado período de tempo *(Executar a cada...)* ou definindo uma data e hora exatas *(Executar a horas específicas)*, ou ainda definindo um evento ao qual a execução da análise esteja associada *(Executar no arranque do computador)*.

- ***Opções de agendamento avançado*** – Esta secção permite-lhe definir em que condições a análise deverá/não deverá ser executada se o computador estiver em modo de baixo consumo ou desligado. Uma vez iniciada a análise agendada à hora especificada, será informado deste facto através de uma janela pop-up aberta no ícone do AVG na barra de tarefas. Será então apresentado um novo ícone do AVG na barra de tarefas (de cor cheia com uma luz intermitente) a informá-lo de que a análise agendada está em execução. Clique com o botão direito do rato no ícone do AVG da análise em execução para abrir um menu de contexto onde pode optar por pausar ou parar a análise em

execução; também pode alterar a prioridade da análise em questão.

Controlos na janela

- ***Guardar*** – Guarda todas as alterações que tiver efetuado neste ou em qualquer outro separador desta janela e volta à síntese de Análises agendadas. Como tal, se pretender configurar os parâmetros de teste em todos os separadores, clique no botão para guardá-los somente após ter especificado todos os requisitos.

- ← – Utilize a seta verde na parte superior esquerda da janela para voltar à síntese de Análises agendadas.

9.4.2. Definições

Na parte superior do separador ***Definições*** pode encontrar o campo de texto no qual pode especificar o nome da análise agendada que está a ser definida. Tente utilizar nomes curtos, descritivos e apropriados de análises para que futuramente seja mais fácil distinguir as análises de outras que venha a definir. Por exemplo, não é adequado identificar uma análise com o nome "Nova análise" ou "A minha análise", uma vez que esses nomes não referem o que a análise efetivamente analisa. Por outro lado, um exemplo de um bom nome descritivo seria "Análise das áreas de sistema", etc.

No separador ***Definições*** encontrará uma lista de parâmetros de análise que podem ser opcionalmente ativados/desativados. ***A menos que tenha uma razão válida para alterar estas definições, recomendamos que mantenha a configuração predefinida***:

- ***Recuperar/remover infeções causadas por vírus sem me perguntar*** *(ativado por predefinição):* se um vírus for detetado durante a análise, pode ser recuperado automaticamente se houver uma cura disponível. Se não for possível recuperar o ficheiro infetado automaticamente, o objeto infetado será movido para a Quarentena de Vírus.

- ***Reportar aplicações potencialmente indesejadas e ameaças de spyware*** *(ativado por predefinição):* marque esta opção para ativar a análise que procura spyware e também vírus. O

Spyware representa uma categoria de malware questionável: apesar de normalmente representar um risco de segurança, alguns destes programas podem ser instalados intencionalmente. Recomendamos que mantenha esta funcionalidade ativada, uma vez que aumenta a segurança do seu computador.

- ***Reportar conjunto avançado de aplicações potencialmente indesejadas*** (*desativado por predefinição*): marque esta opção para detetar pacotes expandidos de spyware: programas que são perfeitamente fidedignos e inofensivos quando adquiridos diretamente ao fabricante, mas que podem ser usados para propósitos maliciosos posteriormente. Esta é uma medida adicional que aumenta a segurança do seu computador ainda mais; no entanto, poderá bloquear programas legais e está, como tal, desativada por predefinição.

- ***Analisar Cookies de Rastreio*** (*desativado por predefinição*): este parâmetro especifica que os cookies deverão ser detetados durante a análise (*os cookies HTTP são utilizados para autenticação, rastreio e manutenção de informação específica dos utilizadores, tal como preferências de sites ou os conteúdos dos carrinhos de compras eletrónicos dos mesmos*).

- ***Pesquisa no interior dos arquivos*** (*desativado por predefinição*): este parâmetro especifica que a análise deverá verificar todos os ficheiros mesmo se estes estiverem comprimidos em arquivos, ex.: ZIP, RAR, etc.

- ***Utilizar Heurística*** (*ativado por predefinição*): a análise heurística (*emulação dinâmica das instruções do objeto analisado num ambiente de computador virtual*) será um dos métodos utilizados para a deteção de vírus durante a análise.

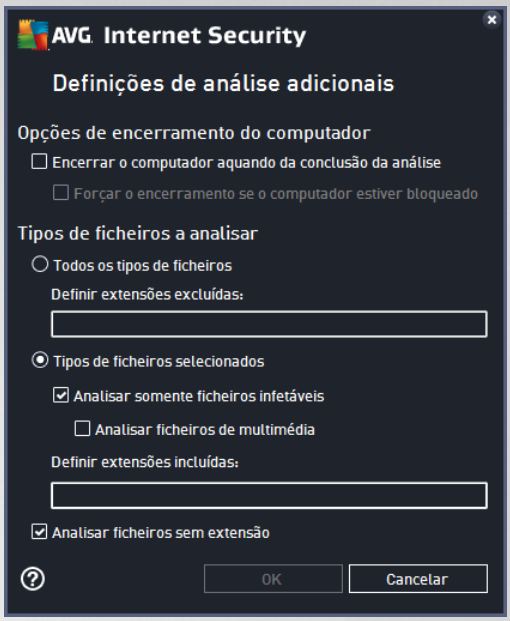
- ***Analisar ambiente de sistema*** (*ativado por predefinição*): a análise verificará também as áreas de sistema do seu computador.

- ***Ativar análise minuciosa*** (*desativado por predefinição):* em situações específicas (*suspeita de infeção do computador*) pode marcar esta opção para ativar os algoritmos de análise mais rigorosos que irão analisar todas as áreas do seu computador, incluindo as que raramente são infetadas, por precaução. Tenha em consideração que este método é bastante demorado.

- ***Analisar rootkits*** *(ativado por predefinição):* a análise Anti-Rootkit analisa o computador para procurar possíveis rootkits, ou seja, programas e tecnologias que podem ocultar atividade de malware no computador. Se for detetado um rootkit, isto não significa necessariamente que o computador esteja infetado. Em alguns casos, podem ser erroneamente detetados controladores específicos ou secções de aplicações seguras como sendo rootkits.

Definições de análise adicionais

A ligação abre uma nova janela de ***Definições de análise adicionais*** onde pode especificar os seguintes parâmetros:


AVG Internet Security
Definições de análise adicionais
Opções de encerramento do computador
Encerrar o computador aquando da conclusão da análise
Forçar o encerramento se o computador estiver bloqueado
Tipos de ficheiros a analisar
Todos os tipos de ficheiros
Definir extensões excluídas:
Tipos de ficheiros selecionados
Analisar somente ficheiros infetáveis
Analisar ficheiros de multimédia
Definir extensões incluídas:
Analisar ficheiros sem extensão
OK
Cancelar

- ***Opções de encerramento do computador*** – decida se o computador deve ser encerrado automaticamente uma vez concluído o processo de análise em execução. Tendo confirmado esta opção *(Encerrar o computador aquando da conclusão da análise)*, será ativada uma nova opção que permite que o computador encerre mesmo que esteja bloqueado *(Forçar o encerramento se o computador estiver bloqueado)*.

- ***Tipos de ficheiros a analisar*** – também deve decidir se pretende analisar:

    - ***Todos os tipos de ficheiros*** com a opção de definir exceções da análise ao indicar uma lista de extensões separadas por vírgula que não devem ser analisadas.

    - ***Tipos de ficheiros selecionados*** – pode especificar que pretende analisar apenas ficheiros que possam ser infetados *(ficheiros que não possam ser infetados não serão analisados, por exemplo, alguns ficheiros de texto simples ou outros ficheiros não executáveis)*, incluindo ficheiros multimédia *(ficheiros de áudio, vídeo – se deixar esta caixa desmarcada, reduzirá o tempo de análise ainda mais, uma vez que os ficheiros são por vezes muito grandes e é pouco provável que estejam infetados por vírus)*. Mais uma vez, pode especificar por extensões os ficheiros que deverão ser sempre analisados.

    - Opcionalmente, pode decidir se pretende ***Analisar ficheiros sem extensão*** – esta opção está ativada por predefinição e é recomendável que a mantenha assim a menos que tenha uma razão válida para a alterar. Os ficheiros sem extensões são bastante suspeitos e devem ser sempre analisados.

Ajustar a rapidez de conclusão de uma Análise

Nesta secção pode ainda especificar a velocidade de análise pretendida consoante a utilização dos recursos do sistema. Por predefinição, o valor desta opção está definido para o nível de *Opção do utilizador* de utilização automática de recursos. Se quiser que a análise seja executada mais rapidamente, esta demorará menos tempo, mas os recursos do sistema utilizados aumentarão significativamente durante a execução da análise e tal diminuirá o desempenho de outras atividades no PC (*esta opção pode ser utilizada quando o seu computador estiver ligado e ninguém o estiver a utilizar*). Por outro lado, pode diminuir os recursos do sistema

utilizados prolongando a duração da análise.

Definir relatórios de análise adicionais

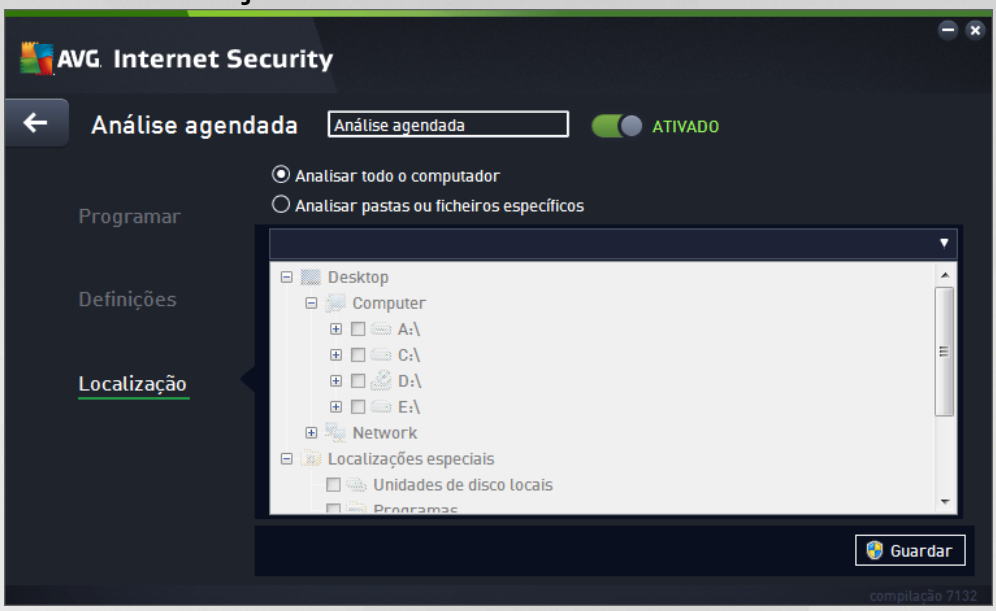
Clique na ligação ***Definir relatórios de análise adicionais...*** para abrir uma janela independente intitulada ***Relatórios de análise***, na qual pode selecionar vários itens para definir quais as deteções que deverão ser reportadas:

Controlos na janela

- ***Guardar*** – Guarda todas as alterações que tiver efetuado neste ou em qualquer outro separador desta janela e volta à síntese de Análises agendadas. Como tal, se pretender configurar os parâmetros de teste em todos os separadores, clique no botão para guardá-los somente após ter especificado todos os requisitos.

- ← – Utilize a seta verde na parte superior esquerda da janela para voltar à síntese de Análises agendadas.

9.4.3. Localização



No separador ***Localização*** pode definir se pretende agendar uma análise de todo o computador ou uma análise de ficheiros ou pastas. Na eventualidade de selecionar a análise de ficheiros ou pastas, a estrutura em árvore apresentada na parte inferior desta janela é ativada e pode especificar as pastas a serem analisadas (*expanda os itens clicando no 'mais' até encontrar a pasta que pretende analisar*). Pode selecionar várias pastas ao selecionar as caixas respetivas. As pastas selecionadas irão aparecer no campo de texto no topo da janela e a lista de opções guardará o histórico das suas análises selecionadas para utilização futura. Em alternativa, pode introduzir a localização completa da pasta pretendida manualmente (*se introduzir várias localizações, é necessário separá-las com ponto e vírgula sem quaisquer espaços adicionais*).

Na estrutura em árvore pode igualmente visualizar uma secção com a identificação ***Localizações especiais***. Em seguida é apresentada uma lista de localizações que serão analisadas se a respetiva caixa estiver marcada:

- ***Unidades de disco locais*** – todas as unidades de disco do seu computador
- ***Ficheiros de Programas***
    - C:\Ficheiros de Programas\
    - *na versão de 64 bits* C:\Ficheiros de Programas (x86)
- ***Pasta Os Meus Documentos***
    - *para o Win XP:* C:\Documents and Settings\Default User\Os Meus Documentos\
    - *para o Windows Vista/7*: C:\Users\utilizador\Documentos\
- ***Documentos Partilhados***
    - *para o Win XP*: C:\Documents and Settings\All Users\Documentos\

- *para o Windows Vista/7*: C:\Users\Public\Documentos\

- ***Pasta Windows*** – C:\Windows\

- ***Outra***

  - *Unidade de sistema* – a unidade de disco rígido na qual o sistema operativo está instalado (normalmente C:)

  - *Pasta de sistema* – C:\Windows\System32\

  - *Pasta dos Ficheiros Temporários* – C:\Documents and Settings\User\Local\ (*Windows XP*); ou C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)

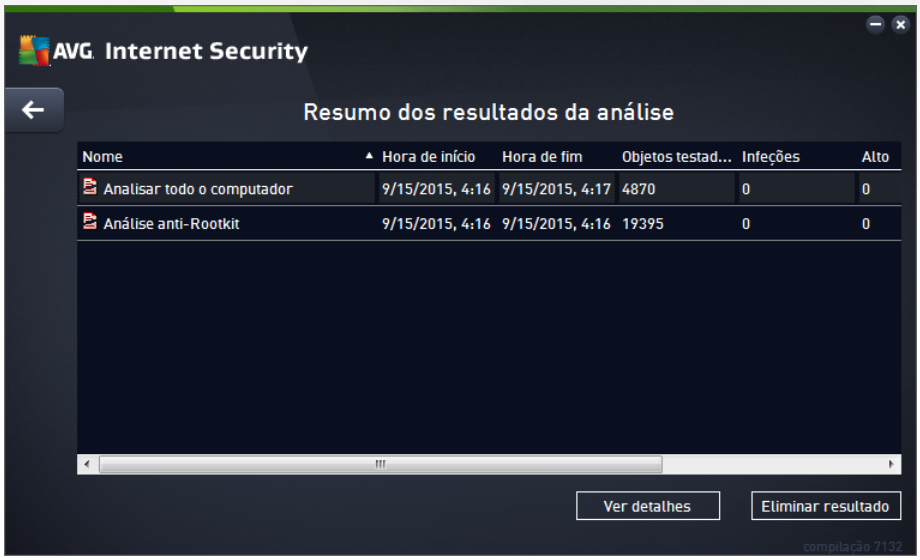
  - *Ficheiros Temporários da Internet* – C:\Documents and Settings\User\Local Settings \Temporary Internet Files\ (*Windows XP*); ou C:\Users\user\AppData\Local\Microsoft\Windows \Temporary Internet Files (*Windows Vista/7*)

Controlos na janela

- ***Guardar*** – Guarda todas as alterações que tiver efetuado neste ou em qualquer outro separador desta janela e volta à síntese de Análises agendadas. Como tal, se pretender configurar os parâmetros de teste em todos os separadores, clique no botão para guardá-los somente após ter especificado todos os requisitos.

- – Utilize a seta verde na parte superior esquerda da janela para voltar à síntese de Análises agendadas.

9.5. Resultados da Análise



A janela ***Resumo dos resultados da análise*** apresenta uma lista com os resultados de todas as análises efetuadas até ao momento. A tabela apresenta a seguinte informação relativa a cada resultado da análise:

- ***Ícone*** – A primeira coluna apresenta um ícone de informação que descreve o estado da análise:
  - Nenhuma infeção detetada, análise concluída
  - Nenhuma infeção detetada, análise interrompida antes da conclusão
  - Foram detetadas infeções que não foram restauradas, análise concluída
  - Foram detetadas infeções que não foram restauradas, análise interrompida antes da conclusão
  - Foram detetadas infeções e todas as infeções foram restauradas ou removidas, análise concluída
  - Foram detetadas infeções e todas as infeções foram restauradas ou removidas, análise interrompida antes da conclusão
- ***Nome*** – A coluna apresenta o nome da análise respetiva. Pode ser uma das duas análises predefinidas ou a sua própria análise agendada.
- ***Hora de início*** – Mostra a data e a hora exatas em que a análise foi iniciada.
- ***Hora de fim*** – Mostra a data e a hora exatas em que a análise foi concluída, interrompida ou parada.
- ***Objetos testados*** – Apresenta o número total de objetos analisados.
- ***Infeções*** – Mostra o número de infeções removidas/o total de infeções detetadas.
- ***Alto / Médio / Baixo*** – As três colunas subsequentes mostram o número de infeções de gravidade alta, média e baixa, respetivamente.
- ***Rootkits*** – Apresenta o número total de rootkits encontrados durante a análise.

Controlos da janela

Ver detalhes – Clique no botão para ver informações detalhadas relativas a uma análise selecionada *(realçada na tabela acima)*.

Eliminar resultados – Clique no botão para remover a informação relativa ao resultado de uma análise selecionada da tabela.

– Utilize a seta verde na parte superior esquerda da janela para voltar à interface de utilizador principal com a síntese dos componentes.

9.6. Detalhes dos Resultados da Análise

Para abrir uma síntese de informações detalhadas relativas ao resultado de uma análise selecionada, clique no botão ***Ver detalhes*** que se encontra na janela Resumo dos resultados da análise. Será redirecionado para a mesma interface que descreve detalhadamente as informações relativas ao resultado de uma análise específica. As informações estão divididas em três separadores:

- ***Resumo*** – O separador apresenta informações básicas relativas à análise: se a análise foi concluída com sucesso, se foram encontradas ameaças e o que foi feito às ameaças.

- ***Detalhes*** – O separador apresenta todas as informações relativas à análise, incluindo detalhes relativos a ameaças detetadas. Exportar síntese para ficheiro permite guardar o resumo como um ficheiro .csv.

- ***Deteções*** – Este separador só aparece se tiverem sido detetadas ameaças durante a análise e apresenta informações detalhadas relativas às ameaças:

  Gravidade informativa: informação ou avisos, não ameaças reais. Normalmente documentos que contêm macros, documentos ou arquivos protegidos por palavra-passe, ficheiros bloqueados, etc.

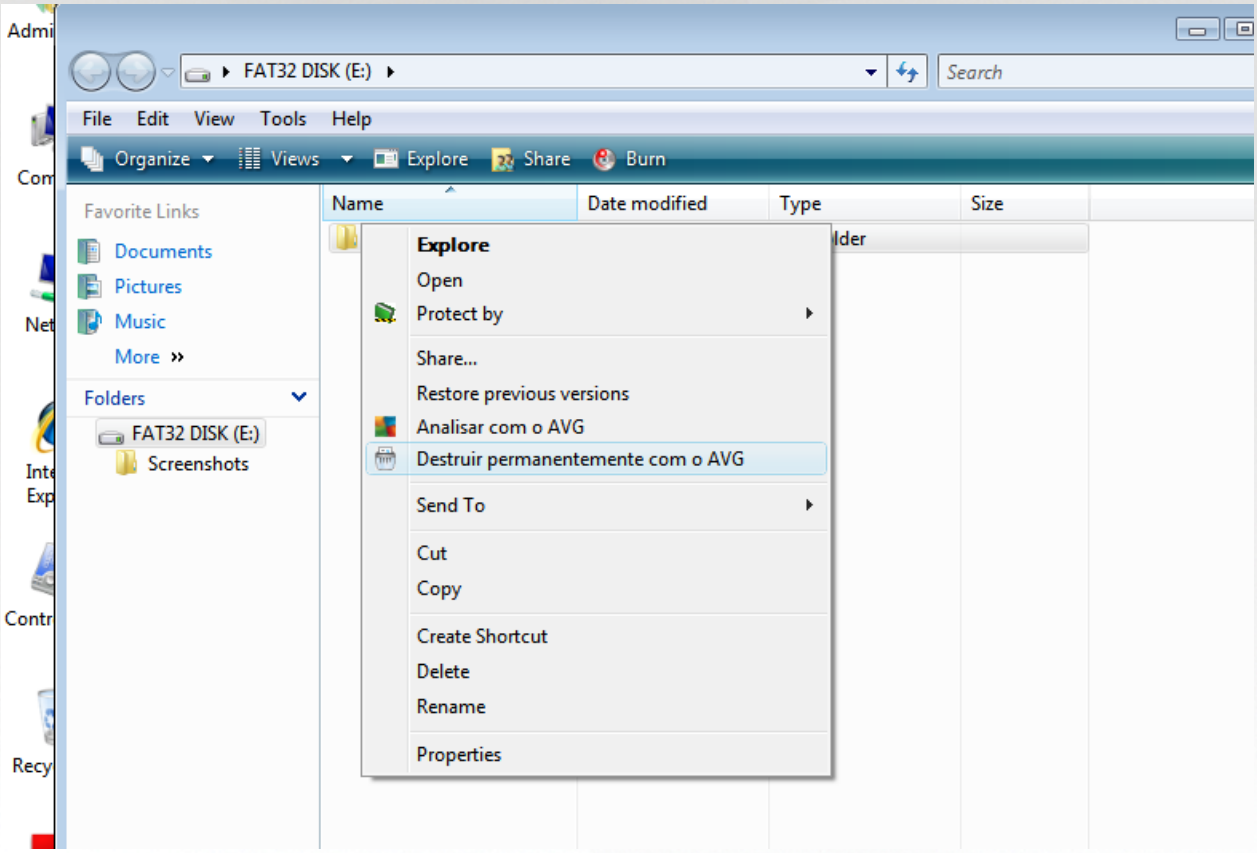
  Gravidade média: normalmente aplicações potencialmente indesejadas *(por exemplo, adware)* ou cookies de rastreio

  Gravidade alta: ameaças graves, tais como vírus, cavalos de Troia, exploits, etc. Inclui também objetos detetados pelo método de deteção da análise heurística, ou seja, ameaças ainda não descritas na base de dados de vírus.

10. AVG File Shredder

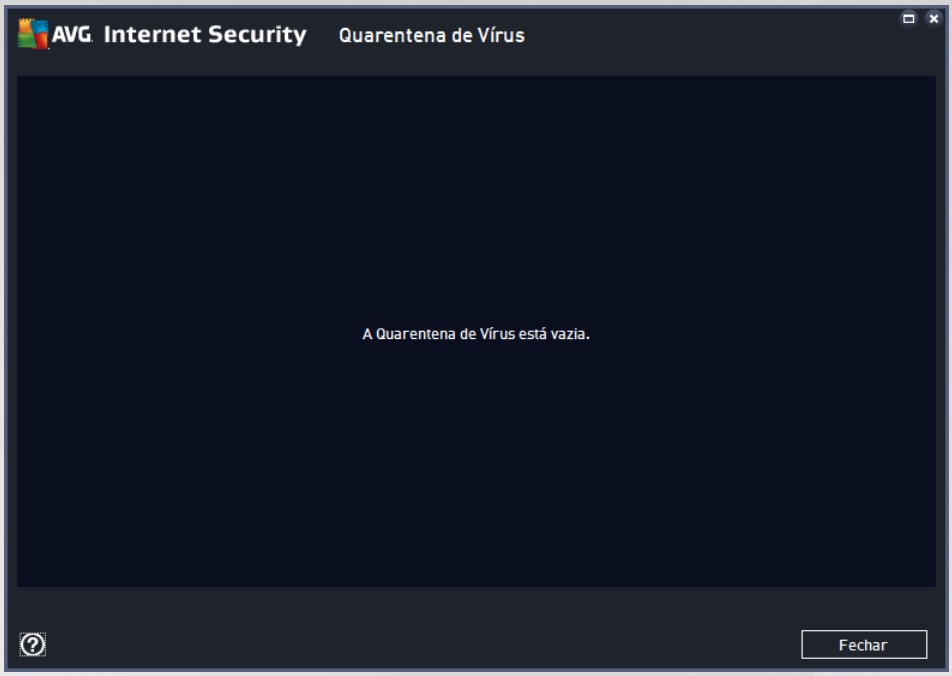
O ***AVG File Shredder*** foi concebido para eliminar ficheiros de forma totalmente segura, ou seja, sem possibilidade de recuperação, mesmo com ferramentas avançadas de software destinadas a esse fim.

Para destruir um ficheiro ou uma pasta, clique com o botão direito do rato no ficheiro ou na pasta num gestor de ficheiros *(Explorador do Windows, Total Commander, etc.)* e selecione ***Destruir permanentemente com o AVG*** no menu de contexto. Também é possível destruir ficheiros contidos na Reciclagem. Se não for possível destruir de forma segura um ficheiro específico numa localização específica *(por exemplo, num CD-ROM)*, receberá uma notificação ou a opção do menu de contexto não estará disponível de todo.



Tenha sempre em atenção que, uma vez destruído um ficheiro, não será possível recuperá-lo.

11. Quarentena de Vírus



A ***Quarentena de Vírus*** é um ambiente seguro para a gestão de objetos suspeitos/infetados detetados durante os testes do AVG. Se um objeto infetado for detetado durante a análise e o AVG não puder recuperá-lo automaticamente, deverá decidir o que fazer com o objeto suspeito. A solução recomendada consiste em mover o objeto para a ***Quarentena de Vírus*** para tratamento futuro. O propósito principal da ***Quarentena de Vírus*** é manter qualquer ficheiro eliminado durante um determinado período de tempo, para que possa certificar-se de que já não necessita do ficheiro na localização original. Se, porventura, descobrir que a ausência do ficheiro causa problemas, pode enviar o ficheiro em questão para análise ou restaurá-lo para a localização original.

A interface da ***Quarentena de Vírus*** abre numa janela separada e oferece uma síntese da informação dos objetos infetados colocados em quarentena:

- ***Data de adição*** – Apresenta a data e a hora em que o ficheiro suspeito foi detetado e removido para a Quarentena de Vírus.
- ***Ameaça*** – Se tiver optado por instalar o componente Identidade dentro do **AVG Internet Security**, será apresentada nesta secção uma identificação gráfica da gravidade da deteção: desde inofensiva *(três pontos verdes)* até muito perigosa *(três pontos vermelhos)*. Também poderá encontrar informações sobre o tipo e a localização original da infeção. A ligação *Mais informações* encaminha-o para uma página que apresenta informações detalhadas sobre a ameaça detetada dentro da enciclopédia de vírus online.
- ***Origem*** – Especifica que componente do **AVG Internet Security** detetou a ameaça respetiva.
- ***Notificações*** – Em casos raros, é possível que apareçam nesta coluna algumas notas com comentários detalhados relativos à ameaça detetada.

Botões de controlo

Os seguintes botões de controlo estão acessíveis a partir da interface da ***Quarentena de Vírus***:

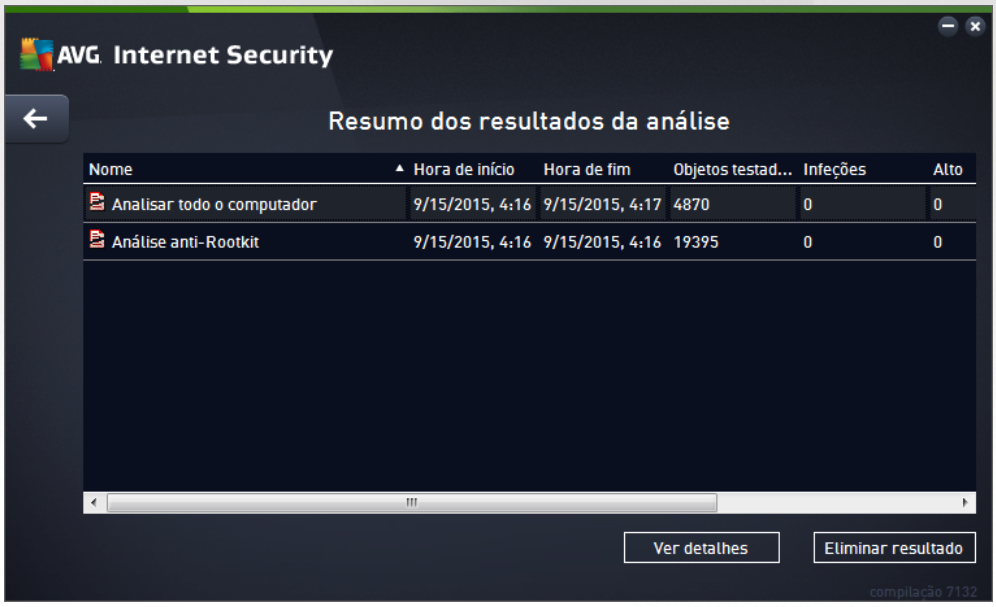
- ***Restaurar*** – repõe o ficheiro infetado na sua localização original no disco rígido.
- ***Restaurar como*** – move o ficheiro infetado para a pasta selecionada.
- ***Enviar para análise*** – o botão só fica ativo quando realça um objeto na lista de deteções acima. Nesse caso, pode optar por enviar a deteção selecionada para os laboratórios de vírus da AVG para uma análise mais detalhada. Tenha em atenção que esta funcionalidade deve servir sobretudo para enviar falsos positivos, ou seja, ficheiros que foram detetados pelo produto AVG como infetados ou suspeitos, mas que o utilizador crê serem inofensivos.
- ***Detalhes*** – para ver informações detalhadas sobre a ameaça específica colocada em quarentena na ***Quarentena de Vírus***, realce o item selecionado na lista e clique no botão ***Detalhes*** para aceder a uma nova janela com a descrição da ameaça detetada.
- ***Eliminar*** – remove o ficheiro infetado da ***Quarentena de Vírus*** completa e irreversivelmente.
- ***Quarentena vazia*** – remove todo o conteúdo da ***Quarentena de Vírus*** completamente. Ao remover os ficheiros da ***Quarentena de Vírus***, esses ficheiros são irremediavelmente removidos do disco (*não movidos para a Reciclagem*).

12. Histórico

A secção ***Histórico*** inclui informações relativas a todos os eventos passados *(tais como atualizações, análises, deteções, etc.)* e os relatórios referentes a esses eventos. É possível aceder a esta secção a partir da interface de utilizador principal através do item ***Opções / Histórico***. O histórico de todos os eventos registados está dividido nas seguintes secções:

- Resultados da Análise
- Resultados da Proteção Residente
- Resultados da Proteção de E-mail
- Resultados da Proteção Online
- Histórico de Eventos
- Registo da Firewall

12.1. Resultados da Análise



É possível aceder à janela ***Resumo dos resultados da análise*** através do item de menu ***Opções / Histórico / Resultados da Análise*** na navegação da linha superior da janela principal do **AVG Internet Security**. A janela faculta uma lista de todas as análises executadas anteriormente e informações relativas aos seus resultados:

- ***Nome*** – designação da análise; pode ser o nome de uma das análises predefinidas ou um nome que tenha atribuído à sua própria análise agendada. Cada nome inclui um ícone que indica o resultado da análise:

  – ícone verde informa que não foram detetadas quaisquer infeções durante a análise

  – ícone azul anuncia que foi detetada uma infeção durante a análise mas que o objeto

infetado foi removido automaticamente

– ícone vermelho avisa que foi detetada uma infeção durante a análise e que não pôde ser removida!

Cada ícone pode ser sólido ou cortado ao meio – o ícone sólido representa uma análise que foi concluída devidamente; o ícone cortado ao meio significa que a análise foi cancelada ou interrompida.

Atenção: *para informações detalhadas de cada análise, consulte a janela Resultados da Análise acessível através do botão Ver detalhes (na parte inferior desta janela).*

- ***Hora de inicio*** – data e hora em que a análise foi iniciada
- ***Hora de fim*** – data e hora em que a análise foi terminada
- ***Objetos testados*** – número de objetos que foram verificados durante a análise
- ***Infeções*** – número de infeções de vírus detetadas/removidas
- ***Alto / Médio*** – estas colunas mostram o número de infeções removidas/o total de infeções detetadas de gravidade alta e média, respetivamente
- ***Informação*** – informações relativas ao decurso da análise e resultado *(normalmente sobre a sua finalização ou interrupção)*
- ***Rootkits*** – número de rootkits

Botões de controlo

Os botões de controlo para a janela ***Resumo dos resultados da análise*** são:

- ***Ver detalhes*** – clique para mudar para a janela Resultados da Análise para ver dados detalhados da análise selecionada
- ***Eliminar resultado*** – clique para remover o item selecionado do resumo dos resultados da análise
- – para voltar à janela principal do AVG predefinida *(síntese de componentes),* utilize a seta que se encontra no canto superior esquerdo desta janela

12.2. Resultados da Proteção Residente

O serviço ***Proteção Residente*** faz parte do componente ***Computador*** e analisa os ficheiros quando são copiados, abertos ou guardados. Quando um vírus ou qualquer tipo de ameaça for detetado, o utilizador será imediatamente notificado através da seguinte janela:

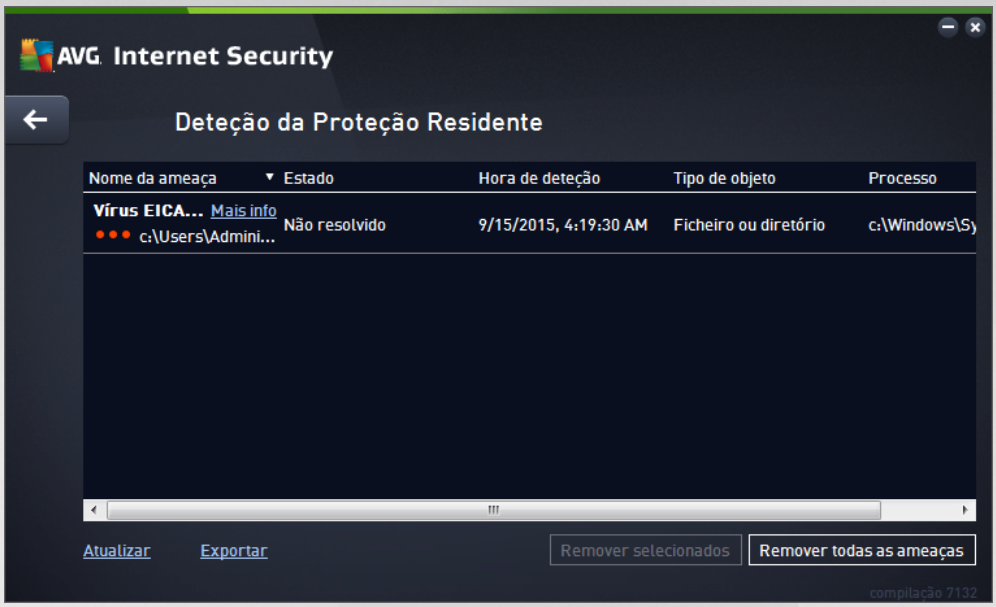
AVG Internet Security
Deteção do AVG
Ameaça:
Vírus EICAR_Test identificado [Mais informações]
Nome do objeto:
c:\Users\Administrator\Documents\EICAR.COM
Proteger-me (recomendado)
A AVG irá escolher o melhor método de remoção desta ameaça.
Ignorar a ameaça
O ficheiro identificado continuará na sua localização atual no disco. Para assegurar que está protegido, o componente Proteção Residente não permitirá o acesso a ficheiros infetados. A ameaça não será removida.
Mostrar detalhes

Nesta janela de aviso encontrará informação relativa ao objeto que foi detetado e considerado infetado (*Ameaça*) e alguns factos descritivos relacionados com a infeção reconhecida (*Descrição*). A ligação *Mais informações* encaminha-o para uma página que apresenta informações detalhadas sobre a ameaça detetada dentro da enciclopédia de vírus online (se a ameaça for conhecida). Na janela também poderá ver uma síntese de soluções disponíveis para o tratamento da ameaça detetada. Uma das alternativas será identificada como sendo recomendada: ***Proteger-me (recomendado). Se possível, deverá sempre selecionar esta opção!***

Nota: *pode acontecer que o tamanho do objeto detetado exceda o limite de espaço livre na Quarentena de Vírus. Se isso acontecer, será informado por meio de um pop-up sobre a questão quando tentar mover o objeto infetado para a Quarentena de Vírus. Contudo, o tamanho da Quarentena de Vírus pode ser modificado. É definido como percentagem ajustável do tamanho real do seu disco rígido. Para aumentar o tamanho da Quarentena de Vírus, aceda à janela Quarentena de Vírus nas Definições Avançadas do AVG e defina-o na opção "Tamanho limite de Quarentena de Vírus".*

Pode encontrar a ligação ***Mostrar detalhes*** na parte inferior da janela. Clique na ligação para abrir uma nova janela com informações detalhadas sobre o processo que estava em execução quando a infeção foi detetada e a identificação do processo.

Está disponível uma lista de todas as deteções da Proteção Residente para revisão na janela ***Deteção da Proteção Residente***. É possível aceder a essa janela através do item de menu ***Opções / Histórico / Deteção da Proteção Residente*** na navegação da linha superior da janela principal do **AVG Internet Security. A janela apresenta uma síntese de objetos que foram detetados pela proteção residente, avaliados como perigosos e recuperados ou movidos para a** Quarentena de Vírus.



É facultada a seguinte informação para cada objeto detetado:

- ***Nome da ameaça*** – descrição (*possivelmente até o nome*) do objeto detetado e respetiva localização. A ligação *Mais informações* encaminha-o para uma página que apresenta informações detalhadas sobre a ameaça detetada dentro da enciclopédia de vírus online.
- ***Estado*** – ação efetuada com o objeto detetado
- ***Hora de deteção*** – data e hora em que a ameaça foi detetada e bloqueada
- ***Tipo de objeto*** – tipo do objeto detetado
- ***Processo*** – que ação foi efetuada para atrair o objeto potencialmente perigoso de forma a este poder ser detetado

Botões de controlo

- ***Atualizar*** – procederá à atualização da lista de deteções da ***Proteção Residente***
- ***Exportar*** – procederá à exportação da lista completa de objetos detetados para um ficheiro
- ***Remover selecionados*** – pode realçar na lista registos selecionados e utilizar este botão para eliminar apenas esses itens selecionados
- ***Remover todas as ameaças*** – utilize este botão para eliminar todos os registos listados nesta janela
- ← – para voltar à janela principal do AVG predefinida *(síntese de componentes),* utilize a seta que se encontra no canto superior esquerdo desta janela

12.3. Resultados da Proteção de Identidade

É possível aceder à janela ***Resultados da Proteção de Identidade*** através do item de menu ***Opções / Histórico / Resultados da Proteção de Identidade*** na navegação da linha superior da janela principal do **AVG Internet Security**.

A janela apresenta uma lista de todas as deteções detetadas pelo componente Proteção de Identidade. É facultada a seguinte informação para cada objeto detetado:

- ***Nome da ameaça*** – descrição *(possivelmente até o nome)* do objeto detetado e respetiva localização. A ligação *Mais informações* encaminha-o para uma página que apresenta informações detalhadas sobre a ameaça detetada dentro da enciclopédia de vírus online.
- ***Estado*** – ação efetuada com o objeto detetado
- ***Hora de deteção*** – data e hora em que a ameaça foi detetada e bloqueada
- ***Tipo de objeto*** – tipo do objeto detetado
- ***Processo*** – que ação foi efetuada para atrair o objeto potencialmente perigoso de forma a este poder ser detetado

Na parte inferior da janela, por baixo da lista, encontrará informações sobre o número total de objetos detetados listados acima. Pode também exportar toda a lista dos objetos detetados para um ficheiro (***Exportar lista para ficheiro***) e eliminar todas as entradas relativas a objetos detetados (***Limpar lista***).

Botões de controlo

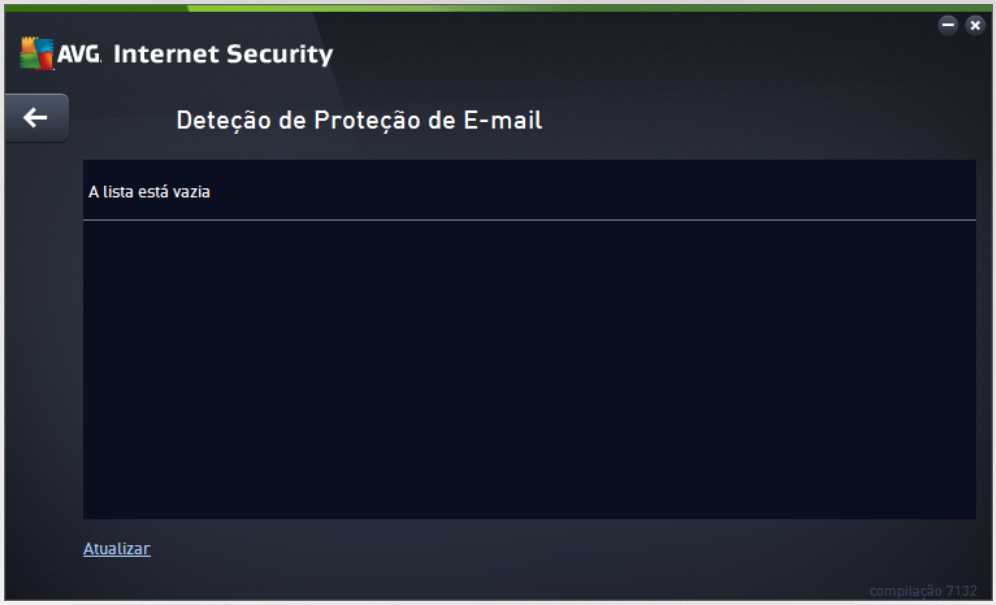
Os botões de controlo disponíveis na interface de ***Resultados da Proteção de Identidade*** são os seguintes:

- ***Atualizar Lista*** – atualiza a lista de ameaças detetadas

- ← – para voltar à janela principal do AVG predefinida *(síntese de componentes),* utilize a seta que se encontra no canto superior esquerdo desta janela

12.4. Resultados da Proteção de E-mail

É possível aceder à janela ***Resultados da Proteção de E-mail*** através do item de menu ***Opções / Histórico / Resultados da Proteção de E-mail*** na navegação da linha superior da janela principal do **AVG Internet Security**.



A janela apresenta uma lista de todas as deteções detetadas pelo componente Verificador de E-mail. É facultada a seguinte informação para cada objeto detetado:

- ***Nome da deteção*** – descrição *(possivelmente até o nome)* do objeto detetado e da sua origem
- ***Resultado*** – ação efetuada com o objeto detetado
- ***Hora de deteção*** – data e hora em que o objeto suspeito foi detetado
- ***Tipo de objeto*** – tipo do objeto detetado
- ***Processo*** – que ação foi efetuada para atrair o objeto potencialmente perigoso de forma a este poder ser detetado

Na parte inferior da janela, por baixo da lista, encontrará informações sobre o número total de objetos detetados listados acima. Pode também exportar toda a lista dos objetos detetados para um ficheiro (***Exportar lista para ficheiro***) e eliminar todas as entradas relativas a objetos detetados (***Limpar lista***).

Botões de controlo

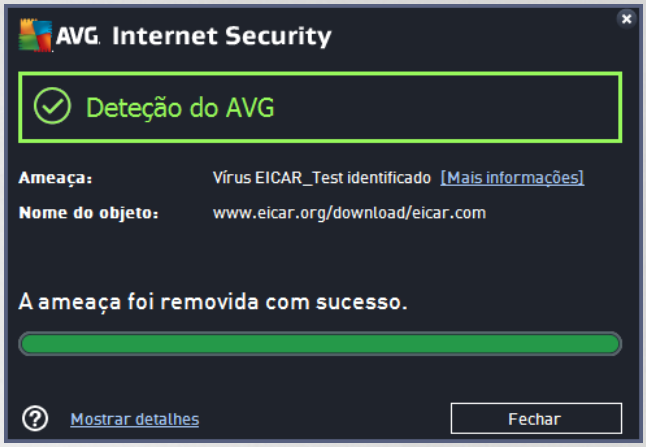
Os botões de controlo disponíveis na interface ***detecção do Verificador de E-mail***são os seguintes:

- ***Actualizar lista*** – actualiza a lista de ameaças detectadas

- ← – para voltar à janela principal do AVG predefinida *(síntese de componentes),* utilize a seta que se encontra no canto superior esquerdo desta janela

12.5. Resultados da Proteção Online

A ***Proteção Online*** analisa o conteúdo de páginas Web visitadas e de possíveis ficheiros incluídos nas mesmas antes de estas serem apresentadas no seu browser ou serem transferidas para o seu computador. Se for detetada uma ameaça, será imediatamente avisado por meio da seguinte janela:



Nesta janela de aviso encontrará informação relativa ao objeto que foi detetado e considerado infetado (*Ameaça*) e alguns factos descritivos relacionados com a infeção reconhecida (*Nome do objeto*). A ligação *Mais informações* redireciona-o para a enciclopédia de vírus online, onde poderá encontrar informações detalhadas sobre a infeção detetada, se a infeção for conhecida. A janela inclui os seguintes elementos de controlo:

- ***Mostrar detalhes*** – clique na ligação para abrir uma nova janela pop-up onde pode encontrar informações sobre o processo em execução quando a infeção foi detetada e a identificação do processo.

- ***Fechar*** – clique no botão para fechar a janela de aviso.

A página Web suspeita não será aberta e a deteção da ameaça será registada na lista de ***Deteções da Proteção Online***. É possível aceder à síntese de ameaças detetadas através do item de menu ***Opções / Histórico / Deteções da Proteção Online*** na navegação da linha superior da janela principal do **AVG Internet Security**.

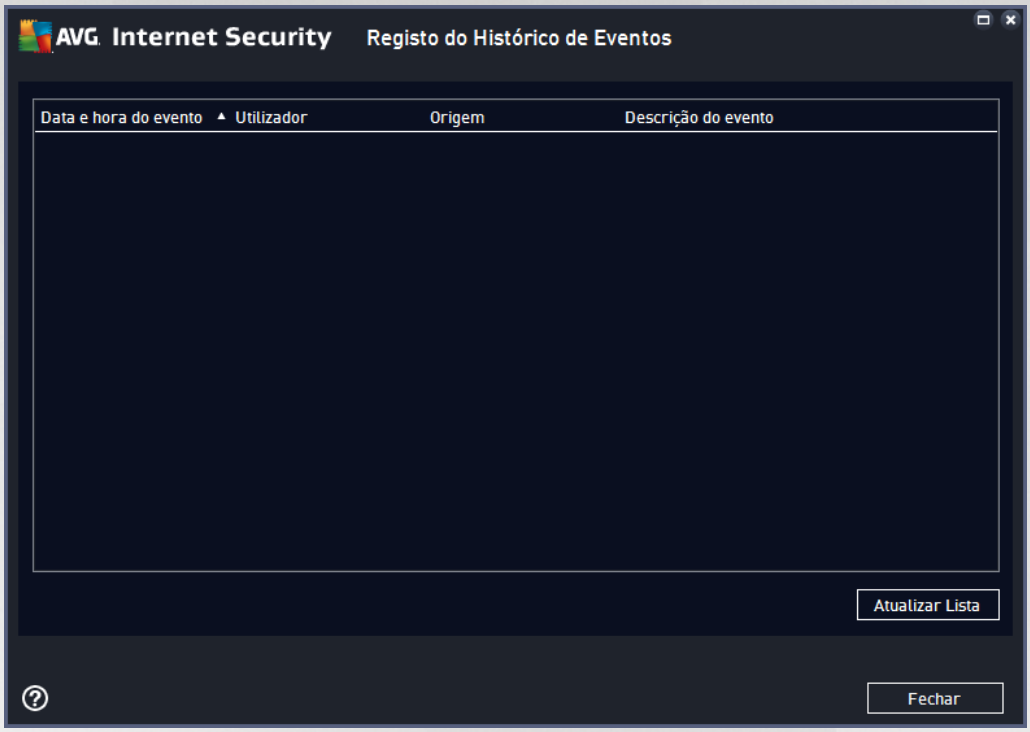
É facultada a seguinte informação para cada objeto detetado:

- ***Nome da ameaça*** – descrição (*possivelmente até o nome*) do objeto detetado e respetiva origem (*página web*); a ligação *Mais informações* encaminha-o para uma página que apresenta informações detalhadas sobre a ameaça detetada dentro da enciclopédia de vírus online.
- ***Estado*** – ação efetuada com o objeto detetado
- ***Hora de deteção*** – data e hora em que a ameaça foi detetada e bloqueada
- ***Tipo de objeto*** – tipo do objeto detetado

Botões de controlo

- ***Atualizar*** – procederá à atualização da lista de deteções da ***Proteção Residente***
- ***Exportar*** – procederá à exportação da lista completa de objetos detetados para um ficheiro
- ← – para voltar à janela principal do AVG predefinida *(síntese de componentes),* utilize a seta que se encontra no canto superior esquerdo desta janela

12.6. Histórico de Eventos



É possível aceder à janela ***Histórico de Eventos*** através do item de menu ***Opções / Histórico / Histórico de Eventos*** na navegação da linha superior da janela principal do **AVG Internet Security**. Nesta janela poderá encontrar um resumo dos eventos importantes ocorridos durante o funcionamento do **AVG Internet Security**. A janela apresenta registos dos seguintes tipos de eventos: informação relativa a atualizações da aplicação AVG; informação relativa ao início, ao fim ou à paragem de análises (*incluindo testes efetuados automaticamente*); informação relativa a eventos relacionados com deteção de vírus (*através da proteção residente ou da análise*), incluindo localização da ocorrência; e outros eventos importantes.

Para cada evento, são apresentadas as seguintes informações:

- ***Data e hora do evento*** apresenta a data e a hora exatas a que o evento ocorreu.
- ***Utilizador*** especifica o nome do utilizador com sessão iniciada no momento em que ocorreu o evento.
- ***Origem*** apresenta a informação relativa ao componente de origem ou a outra parte do sistema AVG que desencadeou o evento.
- ***Descrição do evento*** apresenta um breve resumo do que de facto aconteceu.

Botões de controlo

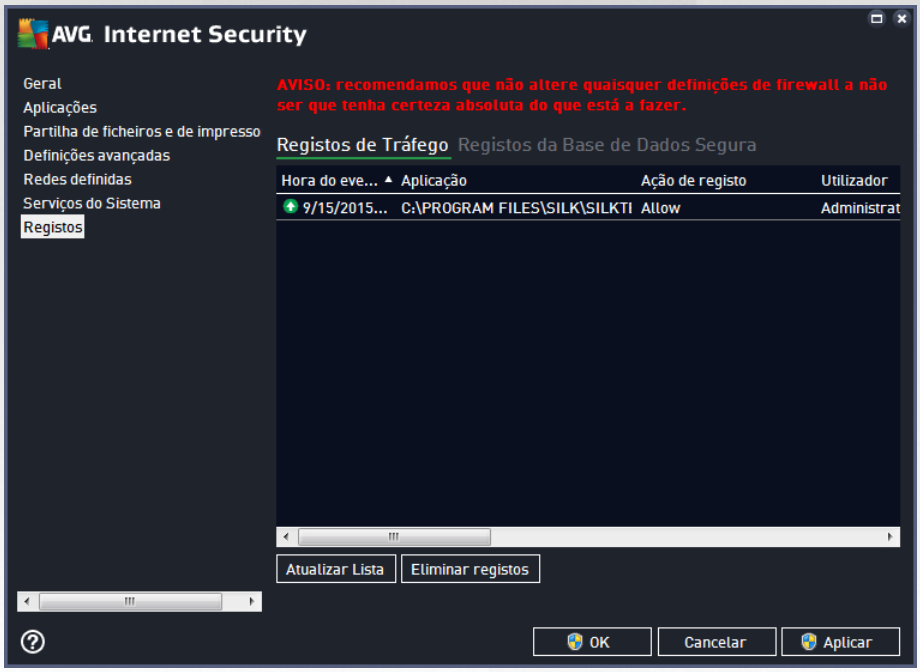
- ***Atualizar lista*** – clique neste botão para atualizar todas as entradas da lista de eventos
- ***Fechar*** – clique neste botão para voltar à janela principal do **AVG Internet Security**

12.7. Registo da Firewall

Esta janela destina-se a configuração avançada e não é recomendável alterar qualquer definição, a menos que tenha a certeza absoluta de que a alteração é necessária!

A janela ***Registos*** permite-lhe rever a lista de todas as ações e eventos da Firewall com uma descrição detalhada de parâmetros relevantes, apresentados em dois separadores:

- ***Registos de Tráfego*** – Este separador apresenta informações relativas às atividades de todas as aplicações que tentaram estabelecer ligação à rede. Para cada item poderá encontrar informações relativas à hora do evento, o nome da aplicação, a ação de registo respetiva, o nome do utilizador, PID, direção do tráfego, tipo de protocolo, os números da porta remota e da porta local e informações relativas ao endereço IP remoto e local.



- ***Registos da Base de Dados Segura*** – A *Base de Dados Segura* é a base de dados interna do AVG que recolhe informações sobre aplicações certificadas e seguras que podem ter sempre permissão para comunicar online. Da primeira vez que uma nova aplicação tentar estabelecer ligação à rede (*ou seja, quando ainda não existe nenhuma regra da firewall especificada para essa aplicação*), é necessário descobrir se a comunicação na rede deve ser permitida para a respetiva aplicação. Primeiro, o AVG procura na *Base de Dados Segura* e, se a aplicação estiver listada, ser-lhe-á concedido acesso à rede automaticamente. Só depois disso, se não houver qualquer informação sobre a aplicação disponível na base de dados, será o utilizador inquirido, por meio de uma janela independente, sobre se pretende que a aplicação aceda à rede.

Botões de controlo

- ***Atualizar lista*** – todos os parâmetros registados podem ser ordenados consoante o atributo selecionado: cronologicamente (*datas*) ou alfabeticamente (*outras colunas*) – basta clicar no cabeçalho da coluna respetiva. Utilize o botão ***Atualizar lista*** para atualizar a informação apresentada.

- ***Eliminar registos*** – clique para eliminar todas as entradas da tabela.

13. Atualizações do AVG

Nenhum software de segurança pode garantir uma proteção efetiva contra vários tipos de ameaças a menos que seja atualizado regularmente! Os criadores de vírus estão constantemente à espreita de novas falhas que possam explorar, tanto em software como nos sistemas operativos. Novos vírus, novo malware, novos ataques de intrusão surgem todos os dias. Por isso, os vendedores de software estão constantemente a lançar atualizações e correções, para solucionar quaisquer falhas de segurança que sejam descobertas.

Tendo em conta todas as novas ameaças informáticas que surgem e a velocidade a que se disseminam, é totalmente essencial atualizar o **AVG Internet Security** regularmente. A melhor solução é manter as configurações predefinidas do programa no caso de estar configurada a atualização automática. Tenha em conta que se a base de dados de vírus do **AVG Internet Security** não estiver atualizada, o programa não poderá detetar as ameaças mais recentes!

É essencial atualizar o seu AVG regularmente! As atualizações de definições de vírus essenciais deverão ser diárias, se possível. As atualizações do programa menos urgentes podem ser semanais.

13.1. Execução de atualização

Para proporcionar o máximo de segurança possível, o **AVG Internet Security** está agendado, por predefinição, para procurar novas atualizações da base de dados de vírus a cada quatro horas. Uma vez que as atualizações do AVG não são lançadas com base num intervalo específico, mas antes em função da quantidade e gravidade das novas ameaças, esta verificação é extremamente importante para garantir que a base de dados de vírus do AVG está constantemente atualizada.

Se quiser verificar a existência de novos ficheiros de atualização imediatamente, utilize o link rápido Atualizar agora na interface de utilizador principal. Este link está constantemente disponível a partir de qualquer janela da interface de utilizador. Assim que inicia a atualização, o AVG verifica a existência de novos ficheiros de atualização disponíveis. Se for o caso, o **AVG Internet Security** começa a transferir os ficheiros e inicia o processo de atualização propriamente dito. Será informado dos resultados da atualização na janela deslizante que aparece por cima do ícone do AVG na barra de tarefas.

Se quiser reduzir o número de execuções da atualização, pode configurar os seus próprios parâmetros de atualização. No entanto, ***recomendamos imperativamente que execute a atualização no mínimo uma vez por dia!*** A configuração pode ser editada na secção Definições avançadas/Agendamentos, especificamente nas seguintes janelas:

- Agendamento de atualização de definições
- Agendamento de atualização do programa
- Agendamento de atualização Anti-Spam

13.2. Níveis de atualização

O **AVG Internet Security** disponibiliza dois níveis de atualização passíveis de seleção:

- ***Atualização de definições*** contém alterações necessárias para uma proteção antivírus, anti-spam e anti-malware fiável. Normalmente, não inclui alterações ao código e apenas atualiza a base de dados de definições. Esta atualização deve ser aplicada logo que esteja disponível.
- ***Atualização do programa*** contém várias alterações, correções e melhoramentos do programa.

Aquando do agendamento de uma atualização, é possível definir parâmetros específicos para ambos os níveis de atualização:

- Agendamento de atualização de definições
- Agendamento de atualização do programa

Nota: *se um agendamento de atualização do programa coincidir com uma análise agendada, o processo de atualização terá precedência e a análise será interrompida. Nesse caso, será informado do conflito.*

14. Perguntas Frequentes e Suporte Técnico

Na eventualidade de ter alguma dúvida ou problema de ordem comercial ou técnica com a sua aplicação **AVG Internet Security**, há várias formas de obter ajuda. Queira escolher entre as seguintes opções:

- ***Obter suporte***: dentro da aplicação AVG, pode aceder a uma página dedicada de apoio ao cliente no website da AVG (*http://www.avg.com/*). Selecione o item ***Ajuda / Obter suporte*** no menu principal para ser encaminhado para o website da AVG com as opções de suporte disponíveis. Para continuar, siga as instruções apresentadas na página.

- ***Suporte*** *(hiperligação do menu principal)*: o menu do AVG (*no topo da interface de utilizador*) inclui a hiperligação ***Suporte*** que abre uma nova janela com todos os tipos de informações de que possa precisar quando procura ajuda. A janela inclui dados básicos sobre o seu programa AVG (*versão do programa/da base de dados*), informações da licença e uma lista de hiperligações de suporte rápido.

- ***Resolução de problemas no ficheiro de ajuda***: está disponível uma nova secção de ***Resolução de problemas*** diretamente no ficheiro de ajuda incluído no **AVG Internet Security** *(para abrir o ficheiro de ajuda, carregue na tecla F1 em qualquer janela da aplicação)*. Esta secção providencia uma lista das situações que ocorrem com maior frequência e que motivam a procura de ajuda profissional por parte de um utilizador. Selecione a situação que melhor descreve o seu problema e clique sobre a mesma para abrir instruções detalhadas que solucionam o problema.

- ***Centro de Suporte do Website da AVG***: em alternativa, pode procurar a solução para o seu problema no website da AVG (*http://www.avg.com/*). Na secção ***Suporte*** pode encontrar uma visão geral de grupos temáticos relacionados com questões técnicas e comerciais, uma secção estruturada de perguntas frequentes e todos os contactos disponíveis.

- ***AVG ThreatLabs***: um site específico associado ao AVG (*http://www.avg.com/about-viruses*) e dedicado a questões relacionadas com vírus, que apresenta uma síntese estruturada de informações relativas a ameaças online. Também encontra instruções para a remoção de vírus, spyware e conselhos sobre como se manter protegido.

- ***Fórum de debate***: também pode usar o fórum de debate dos utilizadores do AVG em http://community.avg.com/.